THE HIDDEN SUBGROUP PROBLEM
FOR GENERALIZED
QUATERNIONS

by

JULIA TUMASOVA UPTON

A DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Mathematics
in the Graduate School of
The University of Alabama

TUSCALOOSA, ALABAMA

2009
ABSTRACT

The hidden subgroup problem is a pivotal problem in quantum computation since it reflects the structure of tasks for which quantum algorithms significantly outperform classical algorithms. In this dissertation, a quantum algorithm that solves the hidden subgroup problem over the generalized quaternion group is developed. The algorithm employs the abelian quantum Fourier transform and Kuperberg sieve to reveal the hidden subgroup.
DEDICATION

I dedicate this dissertation to my grandmother, Tamara Semenovna Babakhanova, an electrical engineer extraordinaire, who showered me with love and inspired my interest in mathematics and science. I love you. I miss you.

I also dedicate this work to my husband Mark, who supported me through every step of this journey. Without you, my love, this would not have been possible.
ACKNOWLEDGMENTS

I would like to thank, first and foremost, my adviser, Dr. Jon Corson, who enthusiastically ventured with me into the exciting new world of quantum computation. Our many discussions of mathematics, physics, technology, and the human condition inspired and guided me throughout this undertaking. I also thank my committee members, Dr. Joseph Neggers, Dr. Martin Evans, Dr. Martyn Dixon, and Dr. Allen Stern for their support.

I am indebted to my family for the constant encouragement, and the sacrifices made to help me succeed in this endeavor. I thank my husband Mark for the inspiration I drew from our numerous discussions and for being there when I needed him most. I am grateful to my daughter Sophia for bringing such joy into my life and making it all worthwhile.
CONTENTS

<table>
<thead>
<tr>
<th>CONTENTS</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>iv</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>viii</td>
</tr>
<tr>
<td>1 INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 The Power of A Quantum Computer</td>
<td>1</td>
</tr>
<tr>
<td>1.2 A Brief History of Quantum Computing</td>
<td>3</td>
</tr>
<tr>
<td>1.3 The Hidden Subgroup Problem in Quantum Computing</td>
<td>4</td>
</tr>
<tr>
<td>1.3.1 General Formulation and Special Cases</td>
<td>4</td>
</tr>
<tr>
<td>1.3.2 The Dihedral Hidden Subgroup Problem</td>
<td>5</td>
</tr>
<tr>
<td>2 A QUANTUM MODEL OF COMPUTATION</td>
<td>6</td>
</tr>
<tr>
<td>2.1 The Quantum Mechanical Framework</td>
<td>6</td>
</tr>
<tr>
<td>2.2 The No-Cloning Theorem</td>
<td>11</td>
</tr>
<tr>
<td>2.3 Quantum Gates</td>
<td>11</td>
</tr>
<tr>
<td>2.3.1 Single-qubit gates</td>
<td>12</td>
</tr>
<tr>
<td>2.3.2 Multi-qubit gates</td>
<td>16</td>
</tr>
<tr>
<td>2.3.3 Universal Quantum Gates</td>
<td>20</td>
</tr>
<tr>
<td>2.4 Probabilistic Nature of Quantum Algorithms</td>
<td>21</td>
</tr>
<tr>
<td>3 SHOR’S FACTORIZATION ALGORITHM</td>
<td>24</td>
</tr>
</tbody>
</table>
LIST OF TABLES

1.1 Special Cases of The Hidden Subgroup Problem . . . . . . . . . . . . . . . . . . . 4
2.1 The AND Operation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 19
2.2 The Chernoff bounds for $\delta = \frac{1}{4}$ . . . . . . . . . . . . . . . . . . . . . . . 23
3.1 Registers’ States . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 32
4.1 Cayley Table for $Q_8$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 47
4.2 Multiplication Table for $Q_8$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 51
4.3 “Twisted” Multiplication . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 52
LIST OF FIGURES

2.1 A Simple Quantum Circuit ........................................ 14
2.2 Hadamard Gates in Parallel ...................................... 15
2.3 CNOT Gate ............................................................. 16
2.4 The Toffoli Gate ....................................................... 19
3.1 Quantum Circuit for $QFT^+$ ...................................... 29
3.2 Quantum Circuit for Period Finding .............................. 29
3.3 Probability Plot ....................................................... 33
3.4 Shor’s Algorithm as a Case of HSP ............................... 35
3.5 Implementable Shor’s Algorithm as a Case of HSP ............ 36
4.1 Quaternion Plaque on Broom Bridge in Dublin ................ 39
4.2 Quantum Circuit for Period Finding over $Q_4$ ............... 44
4.3 Reduction of QHSP ..................................................... 57
CHAPTER 1

INTRODUCTION

Reality is that which, when you stop believing in it, does not go away.

Philip K. Dick

1.1 The Power of A Quantum Computer

A quantum computer is a computing device whose operation is based on the uniquely quantum-mechanical effects of interference and entanglement. The quantum bits (qubits), named after a cubit, an ancient unit of length, are prepared in a superposition of classical computation states which are combined to interfere producing the computation output.

Qubits are manipulated by quantum gates, most of which represent unitary transformations. The general state of a single qubit is a unit vector in a two-dimensional Hilbert space and with a standard choice of the computational basis \{\ket{0}, \ket{1}\} can be written as

$$|\psi\rangle = \alpha \ket{0} + \beta \ket{1} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

(1.1)

where amplitudes \(\alpha\) and \(\beta\) are complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1$$

(1.2)

The state \(|\psi\rangle\) is in a superposition of the states \(|0\rangle\) and \(|1\rangle\), i.e., it exists in both states simultaneously.
The quantum state for a system of $n$ qubits is a unit vector in a $2^n$-dimensional Hilbert space and can be expressed in the computational basis as

$$|\psi^{(n)}\rangle = \sum_{i_0=0}^{1} \cdots \sum_{i_{n-1}=0}^{1} \alpha_{i_0,\ldots,i_{n-1}} |i_0\ldots i_{n-1}\rangle$$

where $|\psi^{(n)}\rangle$ is normalized.

A system of $n$ qubits represents a superposition of $2^n$ states, allowing a quantum computer to operate on states simultaneously. This phenomenon of quantum parallelism is the source of the quantum computer’s overwhelming power that allows for the execution of algorithms which no classical computer can efficiently handle. However, the only way to extract information from qubits is to subject them to measurement, which reduces the system to a single state in accordance with the Born rule. The rule states that for a qubit in a superposition (1.1) the measurement result is 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$. Thus, the post-measurement state no longer contains any information pertaining to the amplitudes of the pre-measurement superposition state, other than indicating that the particular amplitude corresponding to the actual output state was not 0, and likely not exceedingly small. Moreover, a measurement gate is not unitary, i.e., it is irreversible. For an input $x$ covering the range $0 \leq x < 2^n$ and a computed function $f$, the measurement of the input register produces a single randomly chosen $x_0$, while the measurement of the output register gives a single corresponding value $f(x_0)$.

To take advantage of superposition and thus achieve an exponential speedup over the classical computer, quantum algorithms involve judicial arrangements of unitary gates, in some cases supplemented by intermediate measurement gates acting on subsets of a system’s qubits. In most cases, this approach leads to an extraction of information about global properties of $f$, which manifest themselves in the relations between the values of $f$ for many distinct values of $x$, information that a classical computer can only produce by making many independent evaluations.
1.2 A Brief History of Quantum Computing

The Turing machine is the standard mathematical model of a classical computer. A mathematical model of a quantum computer, just as independent of a physical realization, was first discussed by Manin [1] in 1980. A few years later, Feynman [2, 3] pointed out that simulation of certain quantum systems on a classical computer requires time that scales exponentially with the number of particles in a simulated system. Feynman proposed that a quantum system might be efficiently simulated by a computer that exploits quantum effects.

In 1985, a concrete mathematical model, the quantum Turing machine, was introduced by Deutsch [4], who followed it up in 1989 [5] by an equivalent but more convenient model, the quantum circuit. These ideas led to the search for further applications of a quantum computer, initially resulting in solutions to somewhat contrived problems, e.g., the Deutsch-Jozsa algorithm [6], the Simon algorithm [7], and the Bernstein-Varzani algorithm [8]. Nonetheless, these early results demonstrated the existence of specific problems that can be handled dramatically faster by a quantum computer.

A breakthrough that elevated quantum computation from a primarily academic exercise to a matter of great practical significance came in 1994 when Shor [9] introduced polynomial-time quantum algorithms for factoring numbers and computing the discrete logarithm. The widely used public key cryptography systems RSA and Diffie-Hellman rely on the fact that there are no polynomial-time classical algorithms for these problems. When implemented on a quantum computer, Shor’s algorithms will break these encryption schemes in a matter of seconds.

Another masterpiece of quantum-computational software, Grover’s algorithm [10], was introduced in 1996, offering a solution for unstructured search problems with quadratic speedup over classical search algorithms. Recently Hallgren [11] developed a quantum algorithm for Pell’s equation with exponential speedup over any existing classical algorithm.

Quantum algorithms that outperform classical algorithms can be separated into three categories [12]:

1. Algorithms that are based on the quantum Fourier transform (e.g., Shor’s algorithm).
2. Quantum search algorithms.

3. Quantum simulations.

The algorithm developed in this dissertation fits into the first category.

1.3 The Hidden Subgroup Problem in Quantum Computing

1.3.1 General Formulation and Special Cases

The hidden subgroup problem can be stated for any group $G$ as follows.

**Definition 1.3.1.** Let $f : G \rightarrow X$ map a group $G$ to a finite set $X$. Let $H$ be a subgroup of $G$ such that for any $g_1, g_2 \in G$, $f(g_1) = f(g_2)$ if and only if $g_1H = g_2H$.

Determine the generating set of $H$.

Almost all known quantum algorithms that run super-polynomially faster than their classical counterparts also solve special cases of the hidden subgroup problem. Some examples are listed in Table 1.1.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Group $G$</th>
<th>Set $X$</th>
<th>Hidden Subgroup $H$</th>
<th>Function $f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deutsch</td>
<td>$\mathbb{Z}_2$</td>
<td>${0, 1}$</td>
<td>${0}$</td>
<td>$f(0) \neq f(1)$</td>
</tr>
<tr>
<td>Simon</td>
<td>$\mathbb{Z}_n^k$</td>
<td>${0, 1}^n$</td>
<td>${0, s}$, $s \in {0, 1}^n$</td>
<td>$f(s \oplus x) = f(s)$</td>
</tr>
<tr>
<td>Period Finding</td>
<td>$\mathbb{Z}$</td>
<td>any</td>
<td>$r\mathbb{Z}$, $r \in \mathbb{Z}$</td>
<td>$f(x + r) = f(x)$</td>
</tr>
<tr>
<td>Order Finding</td>
<td>$\mathbb{Z}_r \times \mathbb{Z}_r$</td>
<td>${a^k}$, $k \in \mathbb{Z}_r$, $a' = 1$</td>
<td>$r\mathbb{Z}$, $r \in \mathbb{Z}$</td>
<td>$f(x) = a^x$, $f(x + r) = f(x)$</td>
</tr>
<tr>
<td>Discrete logarithm</td>
<td>$\mathbb{Z}_r \times \mathbb{Z}_r$</td>
<td>${a^k}$, $k \in \mathbb{Z}_r$, $a' = 1$</td>
<td>${(t, -ts)}$, $t \in \mathbb{Z}_r$, $s \in \mathbb{Z}_r$</td>
<td>$f(x_1, x_2) = a^{kx_1 + x_2}$, $f(x_1, x_2) = f(x_1 + t, x_2 - ts)$</td>
</tr>
</tbody>
</table>
1.3.2 The Dihedral Hidden Subgroup Problem

**Definition 1.3.2.** The dihedral hidden subgroup problem is the hidden subgroup problem with $G = D_N$, where $D_N$ is the dihedral group of order $2N$

$$D_N = \{ x, y \mid x^N = y^2 = yxyx = 1 \} \quad (1.4)$$

The set of all integral linear combinations of a set of $n$ linearly independent vectors in $\mathbb{R}^n$ is called a lattice. The problem of finding the shortest vector in a lattice is referred to as the unique shortest vector problem. The Ajtai-Dwork public key cryptosystem [13] is based on the hardness of this problem. It has been shown [14] that if there exists a solution to the dihedral hidden subgroup problem that samples cosets, then there exists a quantum algorithm that solves the poly(n)-unique shortest vector problem.

Ettinger and Hoyer [15] developed a quantum algorithm that produces output sufficient to solve the dihedral hidden subgroup problem. However, in this case exponential time is required to reconstruct the hidden subgroup from the output.

The fastest known quantum algorithm for the dihedral hidden subgroup problem was introduced in 2003 by Kuperberg [16]. This approach uses time and query complexity of $2^{O(\sqrt{\log N})}$, where $N$ corresponds to the parameter of underlying group $D_N$. Unfortunately, Kuperberg’s algorithm also requires $2^{O(\sqrt{\log N})}$ quantum space. Another subexponential-time algorithm is due to Regev [17], whose modification of Kuperberg’s approach resulted in a polynomial-space algorithm at a price of a slow-down in time complexity. In this dissertation, a quantum algorithm that solves the hidden subgroup problem for the generalized quaternion group is developed.
CHAPTER 2
A QUANTUM MODEL OF COMPUTATION

2.1 The Quantum Mechanical Framework

Quantum mechanics emerged as a mathematical model for physics to address problems encountered by classical theories in their attempts to explain the results of certain experiments. The following four postulates define the content of quantum mechanics.

**Postulate 1 (State Space).** The state space of a system is a Hilbert space, and the system is completely described by its state vector, a unit vector in the system’s state space. A single qubit constitutes a two-level system whose state is described by a vector in a two-dimensional Hilbert space. Any two vectors with the same global phase are equivalent.

**Postulate 2 (State Evolution).** The evolution of a closed system is described by a unitary transformation. That is, for any evolution of the closed system there exists a unitary operator \( U \) such that if the system is in the state \( |\psi_1\rangle \) at time \( t_1 \), then its state at time \( t_2 \) is

\[
|\psi_2\rangle = U |\psi_1\rangle. \tag{2.1}
\]

A closed quantum system evolves in accordance with the Schrödinger equation

\[
 i\hbar \frac{\partial}{\partial t} |\psi(t_1)\rangle = H |\psi(t_1)\rangle, \tag{2.2}
\]

where \( \hbar \) is the reduced Planck’s constant, and \( H \) is the Hamiltonian, an operator that corresponds to the total energy of the system. The eigenvalues of \( H \) are the possible energies of the system.
For a time-independent Hamiltonian, the state of the system at a later time $t_2$ is given by

$$|\psi(t_2)\rangle = e^{-iHt_2/\bar{h}} |\psi(t_1)\rangle.$$  \hspace{1cm} (2.3)

Thus, the time evolution of the system is governed by the unitary operator

$$U = e^{-iHt/\bar{h}}.$$ \hspace{1cm} (2.4)

The defining relation for any unitary operator $U$ is

$$UU^\dagger = U^\dagger U = I,$$ \hspace{1cm} (2.5)

where $U^\dagger$ denotes the adjoint of $U$.

Since a quantum computer is an $n$-qubit quantum system, the time evolution of its wave function obeys the Schrödinger equation and is described by a unitary operator. In quantum computation, unitary operators are implemented as unitary gates.

**Postulate 3 (State Combination).** The state space of a composite system is the tensor product of the state spaces of its component systems. Given $n$ systems in the states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$, the state of their combined system is

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_1\psi_2\ldots\psi_n\rangle.$$ \hspace{1cm} (2.6)

If $\mathcal{H}_1$ and $\mathcal{H}_2$ are Hilbert spaces of dimensions $N_1$ and $N_2$, respectively, then their tensor product

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$$ \hspace{1cm} (2.7)

has dimension

$$\dim(\mathcal{H}) = N_1N_2.$$ \hspace{1cm} (2.8)
If $\mathcal{H}_1$ and $\mathcal{H}_2$ are endowed with bases $|u_i\rangle$ and $|v_i\rangle$, respectively, then the basis for $\mathcal{H}$ is given by

$$|\omega_i\rangle = |u_i\rangle \otimes |v_i\rangle.$$  \hfill (2.9)

Arbitrary vectors $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$ are expressed as

$$|\psi_1\rangle = \sum_i \alpha_i |u_i\rangle$$
$$|\psi_2\rangle = \sum_i \beta_i |v_i\rangle$$ \hfill (2.10)

with their tensor product $|\phi\rangle \in \mathcal{H}$ given by

$$|\phi\rangle = \sum_{i,j} (\alpha_i \beta_j) |u_i\rangle \otimes |v_j\rangle.$$ \hfill (2.11)

The map

$$\otimes : (\psi_1, \psi_2) \mapsto \psi_1 \otimes \psi_2$$ \hfill (2.12)

is linear in both $\psi_1$ and $\psi_2$.

We can also form a tensor product of operators. Let $U_1$ be an operator that acts on $|\psi_1\rangle \in \mathcal{H}_1$, and let $U_2$ be an operator that acts on $|\psi_2\rangle \in \mathcal{H}_2$. The action of $U_1 \otimes U_2$ on $|\phi\rangle \in \mathcal{H}$ is defined by

$$(U_1 \otimes U_2) |\phi\rangle = (U_1 \otimes U_2) (|\psi_1\rangle \otimes |\psi_2\rangle) = U_1 |\psi_1\rangle \otimes U_2 |\psi_2\rangle.$$ \hfill (2.13)

Operators may be specified in the matrix form relative to some orthonormal basis as

$$U_1 = \sum_{j,k} \alpha_{jk} |j\rangle \langle k| \quad \text{where} \quad \alpha_{jk} = \langle j| U_1 |k\rangle,$$ \hfill (2.14)
$$U_2 = \sum_{j,k} \beta_{jk} |j\rangle \langle k| \quad \text{where} \quad \beta_{jk} = \langle j| U_2 |k\rangle,$$ \hfill (2.15)

where

$$\langle j| = |j\rangle^\dagger.$$ \hfill (2.16)
Their tensor product $U = U_1 \otimes U_2$ can also be expressed in matrix form.

**Definition 2.1.1.** The tensor product of $r \times s$ and $l \times m$ matrices

$$A = \begin{pmatrix}
a_{11} & a_{12} & \ldots & a_{1s} \\
a_{21} & a_{22} & \ldots & a_{2s} \\
\vdots & \vdots & \ddots & \vdots \\
a_{r1} & a_{r2} & \ldots & a_{rs}
\end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix}
b_{11} & b_{12} & \ldots & b_{1m} \\
b_{21} & b_{22} & \ldots & b_{2m} \\
\vdots & \vdots & \ddots & \vdots \\
b_{l1} & b_{l2} & \ldots & b_{lm}
\end{pmatrix}$$

is an $rl \times sm$ matrix defined as

$$A \otimes B = \begin{pmatrix}
a_{11}B & a_{12}B & \ldots & a_{1s}B \\
a_{21}B & a_{22}B & \ldots & a_{2s}B \\
\vdots & \vdots & \ddots & \vdots \\
a_{r1}B & a_{r2}B & \ldots & a_{rs}B
\end{pmatrix}. \quad (2.17)$$

If $A$ and $B$ are unitary, then so is $A \otimes B$. Not all $rl \times sm$ matrices can be represented as tensor products of an $r \times s$ matrix and an $l \times m$ matrix, since an $rl \times sm$ matrix possesses $rslm$ degrees of freedom, while an $r \times s$ matrix and an $l \times m$ matrix have a total of $rs + lm$, and for large enough $r,s,l,m$

$$rslm \gg rs + lm. \quad (2.17)$$

It is possible to decompose the state of an $n$–qubit system into a tensor product of its component states if each of the $n$ qubits forms a closed system. However, if the qubits are allowed to interact, it may not be possible to write the composite state as a product. In this case, the qubits become entangled, i.e., their properties become correlated regardless of spatial separation. A separable state of $n$ qubits depends on $2n$ real parameters, while the entangled state has $2(2^n - 1)$ degrees of freedom.
Postulate 4 (State Measurement). Quantum measurements are described by a collection \( \{ M_m \} \) of measurement operators that act on the state space of a measured system, where \( m \) is an index that corresponds to a possible measurement result. If the system is in the state \( |\psi\rangle \) immediately prior to the measurement, then the probability of measuring a particular outcome \( m \) is given by

\[
\text{Pr}(m) = \langle \psi | M_m^\dagger M_m |\psi\rangle
\]  
(2.18)

and the post-measurement state of the system is

\[
|\psi'\rangle = \frac{M_m |\psi\rangle}{\sqrt{\text{Pr}(m)}}.
\]  
(2.19)

Measurement operators satisfy a completeness relation

\[
\sum_m M_m^\dagger M_m = I.
\]  
(2.20)

In essence, the act of measurement “collapses” the wave function, returning one result that depends on the measurement basis and destroying all the other information about the state. The goal of a quantum algorithm is to produce the most “telling” measurement result, i.e., the one from which the most information can eventually be extracted.
2.2 The No-Cloning Theorem

One of the limitations of a quantum computing model arises from the No-Cloning Theorem proved by Dieks [20], and Wootters and Zurek [21].

**Theorem 2.2.1.** *It is impossible to build a machine that performs unitary transformations and is able to enact the evolution*

\[
|\psi\rangle \otimes |\phi\rangle \longrightarrow |\psi\rangle \otimes |\psi\rangle
\]  

*for an arbitrary state $|\psi\rangle$ and some target state $|\phi\rangle$.*

**Proof.** Suppose there exists a unitary transformation $U$ such that

\[
U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle.
\]  

By linearity of $U$

\[
U(\alpha|\psi\rangle \otimes |\phi\rangle) = \alpha(U(|\psi\rangle \otimes |\phi\rangle)) = \alpha|\psi\rangle \otimes |\psi\rangle.
\]  

Let $|\chi\rangle = \alpha|\psi\rangle$. Then from Eq (2.22) it follows that

\[
U(|\chi\rangle \otimes |\phi\rangle) = |\chi\rangle \otimes |\chi\rangle = \alpha|\psi\rangle \otimes \alpha|\psi\rangle
\]

\[
= \alpha^2|\psi\rangle \otimes |\psi\rangle
\]  

which contradicts Eq (2.23).

\[\square\]

2.3 Quantum Gates

To perform a quantum computation, it is necessary to:

1. Prepare the quantum computer in a well-defined initial state, for example, $|00\ldots0\rangle$.
2. Manipulate the quantum-computer wave function via unitary transformations.
3. Perform a measurement in the computational basis at the end of an algorithm.

The evolution of an $n$-qubit system is described by a unitary matrix of degree $2^n$, but any
such matrix can be decomposed into a product of unitary operations on one or two qubits, and these operations are the elementary quantum gates of the quantum circuit model of computation. It follows from linearity that the action of a gate is completely specified by its action on the computational basis \{|0\rangle, |1\rangle\}.

2.3.1 Single-qubit gates

A quantum gate acting on a single qubit is represented by a $2 \times 2$ unitary matrix. The simplest single-qubit transformation is the identity $I$ whose action on the computational basis is defined by
\[
I : |0\rangle \mapsto |0\rangle, \quad |1\rangle \mapsto |1\rangle
\]  
(2.25)
with the matrix representation
\[
I = |0\rangle \langle 0| + |1\rangle \langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\]  
(2.26)

The quantum NOT gate implements the mapping
\[
X : |0\rangle \mapsto |1\rangle, \quad |1\rangle \mapsto |0\rangle
\]  
(2.27)
and is represented by the matrix
\[
X = |1\rangle \langle 0| + |0\rangle \langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x.
\]  
(2.28)

Similarly,
\[
Y : |0\rangle \mapsto -|1\rangle, \quad |1\rangle \mapsto |0\rangle
\]  
(2.29)
is represented by
\[ Y = |0\rangle \langle 1| - |1\rangle \langle 0| = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\sigma_y, \quad (2.30) \]
and
\[ Z : |0\rangle \mapsto |0\rangle, |1\rangle \mapsto -|1\rangle \quad (2.31) \]
has a representation
\[ Z = |0\rangle \langle 0| - |1\rangle \langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z. \quad (2.32) \]
The matrices \( \sigma_x, \sigma_y, \sigma_z \) are Pauli matrices used in quantum mechanics to describe the spin of a spin-1/2 particle in three spatial dimensions.

The Z gate is a special case (with \( \theta = \pi \)) of the phase shift gate \( P \) that alters the relative phase of the amplitudes of a qubit:
\[ P : |0\rangle \mapsto |0\rangle, |1\rangle \mapsto e^{i\theta} |1\rangle \quad (2.33) \]
\[ P = |0\rangle \langle 0| + e^{i\theta} |1\rangle \langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad (2.34) \]
Other special cases of interest include the S gate with \( \theta = \frac{\pi}{2} \) whose matrix is given by
\[ S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad (2.35) \]
and the T gate with \( \theta = \frac{\pi}{4} \):
\[ T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \quad (2.36) \]
A variation of the phase gate is the discrete phase gate $R_k$ given by

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2k}} \end{pmatrix}$$ (2.37)

A gate used to create superposition states is the Hadamard gate $H$ specified by

$$H = \frac{1}{\sqrt{2}} (|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| - |1\rangle \langle 1|).$$ (2.38)

The action of $H$ on the computational basis is given by

$$H : \begin{cases} |0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{cases}$$ (2.39)

with a representation

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ (2.40)

In the quantum circuit notation, a qubit is denoted by a single line, called a quantum wire, which represents a qubit that is not evolving, i.e., a qubit acted upon by the identity operator $I$. If a qubit is initialized into a particular state, the state is written on the left of the appropriate quantum wire, and if a qubit is to be subjected to a particular unitary transformation, a corresponding gate symbol is placed along the quantum wire. For example, the process of initializing a qubit to a state $|0\rangle$, acting upon it by $H$, and measuring it in the computational basis is denoted by the circuit in Figure 2.1.

**Figure 2.1: A Simple Quantum Circuit**

\[ |0\rangle \quad H \quad \]
Application of a Hadamard gate to an arbitrary qubit $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ yields the state

$$H|\psi\rangle = \alpha H|0\rangle + \beta H|1\rangle = \alpha \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \beta \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \left(\frac{\alpha + \beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha - \beta}{\sqrt{2}}\right)|1\rangle = |\chi\rangle.$$ (2.41)

If a Hadamard gate is now applied to $|\chi\rangle$, we get

$$H|\chi\rangle = \left(\frac{\alpha + \beta}{\sqrt{2}}\right)H|0\rangle + \left(\frac{\alpha - \beta}{\sqrt{2}}\right)H|1\rangle$$

$$= \left(\frac{\alpha + \beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha - \beta}{\sqrt{2}}\right)|1\rangle = \alpha |0\rangle + \beta |1\rangle = |\psi\rangle.$$ (2.42)

Thus, two Hadamard gates applied in series restore a qubit to its original state.

What if two Hadamard gates are applied in parallel, as shown in Figure 2.2?

In this case,

$$(H \otimes H)|0\rangle \otimes |0\rangle = H^{\otimes 2}|0\rangle \otimes |0\rangle = (H|0\rangle)(H|0\rangle)$$

$$= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$ (2.43)
In general, for \( n \in \mathbb{N} \)

\[
H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.
\] (2.44)

### 2.3.2 Multi-qubit gates

Single-qubit gates cannot generate entanglement, as qubit interaction is required to produce an entangled state. An exponential speedup cannot be achieved by a quantum computer that does not exploit entanglement, so we now turn to exploration of multi-qubit gates.

An important set of gates in quantum computation are controlled gates that implement an IF-THEN construct. An example is the 2-qubit controlled NOT, or CNOT gate, depicted in Figure 2.3, where \(\oplus\) is the exclusive-OR operation (binary addition modulo 2).

![Figure 2.3: CNOT Gate](image)

The CNOT gate flips the state of the target qubit if the control qubit is in the state \(|1\rangle\), and acts trivially if the control is in the state \(|0\rangle\), i.e., it implements the following mapping

\[
\text{CNOT} : |00\rangle \mapsto |00\rangle, \quad |01\rangle \mapsto |01\rangle, \quad |10\rangle \mapsto |11\rangle, \quad |11\rangle \mapsto |10\rangle
\] (2.45)
with its transfer matrix given by

\[
\text{CNOT} : = |00\rangle \langle 00| + |01\rangle \langle 01| + |11\rangle \langle 10| + |10\rangle \langle 11|
\]

\[
= |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes X
\]

\[
= \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

\[\text{(2.46)}\]

The CNOT gate can generate entangled states, i.e., states that cannot be decomposed into a tensor product of other states. Consider

\[
\text{CNOT} \left( \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) |0\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle.
\]

\[\text{(2.48)}\]

Suppose the state

\[
|\psi\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle
\]

\[\text{(2.49)}\]

is separable, i.e., there exist \(\alpha, \beta, \gamma, \delta \in \mathbb{C}\) such that

\[
|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle
\]

\[
= (\alpha |0\rangle + \beta |1\rangle) \otimes (\gamma |0\rangle + \delta |1\rangle)
\]

\[
= \alpha \gamma |00\rangle + \beta \gamma |10\rangle + \alpha \delta |01\rangle + \beta \delta |11\rangle
\]

\[\text{(2.50)}\]

But then

\[
\begin{cases}
\alpha \delta = \beta \gamma = 0 \\
\alpha \gamma = \beta \delta = \frac{1}{\sqrt{2}}
\end{cases}
\]

\[\text{(2.51)}\]

which is clearly impossible.
In general, a 2-qubit state

\[ |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} \]  

is separable if and only if

\[ \alpha \delta = \beta \gamma. \]  

(2.53)

The effects of entanglement are clearly demonstrated when measurements are performed. If a measurement of the second qubit of the state \( |\psi\rangle \) results in 0, then the post-measurement state of the system is \( |00\rangle \). The measurement of one qubit of an entangled state affects the probability amplitude of the other qubits in the system.

The CNOT gate can be extended to \( n \) qubits controlling the reversal of the target one. The CCNOT (Controlled-Controlled-NOT) gate, also known as the Toffoli gate, has two control qubits and flips the target qubit only if both controls are in the state \( |1\rangle \).

\[
\text{CCNOT} : = |000\rangle \langle 000| + |001\rangle \langle 001| + |010\rangle \langle 010| + |011\rangle \langle 011| \\
+ |100\rangle \langle 100| + |101\rangle \langle 101| + |110\rangle \langle 110| + |111\rangle \langle 111| \\
= (|00\rangle \langle 00| + |01\rangle \langle 01| + |10\rangle \langle 10|) \otimes I + |11\rangle \langle 11| \otimes X
\]  

(2.54)
The Toffoli gate is shown in Figure 2.4, with the AND operation $\wedge$ defined in Table 2.1.

![Figure 2.4: The Toffoli Gate](image)

$control \mid x \rangle \rightarrow \mid x \rangle$

$control \mid y \rangle \rightarrow \mid y \rangle$

$target \mid z \rangle \rightarrow \mid z \oplus (x \wedge y) \rangle$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>$x \wedge y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 2.1: The AND Operation

The phase shift can be implemented as a controlled transformation

$$CP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}.$$ (2.55)

where the phase shift is applied to the target only when the control qubit is in the state $\mid 1 \rangle$.

An important ingredient in many quantum circuits is the controlled discrete phase gate $CR_k$ described by

$$CR_k : = \mid 00 \rangle \langle 00 \mid + \mid 01 \rangle \langle 01 \mid + \mid 10 \rangle \langle 10 \mid + e^{\frac{2\pi i}{2^k}} \mid 11 \rangle \langle 11 \mid$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}.$$ (2.56)
2.3.3 Universal Quantum Gates

In classical computation, complicated transformations are implemented as a sequence of simpler operations selected from a set of elementary gates. For example, any logical circuit can be simulated using only the AND and the NOT gate, and so these two gates form a set of universal logical gates. In quantum computation, a circuit designer can similarly rely on universal quantum gates.

However, due to the probabilistic nature of quantum computation, a unitary transformation $V$ approximates a desired unitary transformation $U$ to a specified level of accuracy [22], with the approximation error defined by

$$E(U, V) = \max_{|\psi\rangle} \| (U - V)|\psi\rangle \|$$  \hspace{1cm} (2.57)

where

$$||\chi|| = \sqrt{\langle \chi | \chi \rangle}.$$  \hspace{1cm} (2.58)

**Theorem 2.3.1.** The errors of approximating a series of unitary gates $U_1, \ldots, U_n$ by unitary transformations $V_1, \ldots, V_n$ add, so that

$$E(U_nU_{n-1}\ldots U_1, V_nV_{n-1}\ldots V_1) \leq E(U_n, V_n) + E(U_{n-1}, V_{n-1}) + \cdots + E(U_1, V_1)$$  \hspace{1cm} (2.59)

**Proof.** Suppose the desired unitary transformation $U_2U_1$ is implemented by a unitary transformation $V_2V_1$. Then

$$E(U_2U_1, V_2V_1) = \max_{|\psi\rangle} \| (U_2U_1 - V_2V_1)|\psi\rangle \|$$

$$= \max_{|\psi\rangle} \| (U_2U_1 - V_2U_1 + V_2U_1 - V_2V_1)|\psi\rangle \|$$  \hspace{1cm} (2.60)

$$= \max_{|\psi\rangle} \| (U_2 - V_2)U_1|\psi\rangle + V_2(U_1 - V_1)|\psi\rangle \|.$$
Since $U_1$ and $V_2$ are unitary,

$$E(U_2 U_1, V_2 V_1) \leq E(U_2, V_2) + E(U_1, V_1).$$  \hspace{1cm} (2.61)$$

and the result follows by induction.

If a unitary transformation is to be implemented to a precision $\varepsilon$ with $N$ gates, it is only necessary to implement each gate to a precision of $\frac{\varepsilon}{N}$.

It has been shown that all quantum circuits can be constructed by using only CNOT and single-qubit gates [27], which brings us to a definition of a universal quantum gate set.

**Definition 2.3.2.** A set of gates $\mathcal{G}$ is a universal quantum gate set if for every $\varepsilon > 0$, $n \in \mathbb{N}$, any $n$–qubit unitary operator can be approximated to an accuracy $\varepsilon$ by a finite sequence of gates from set $\mathcal{G}$.

The universal gate sets commonly used in quantum computation are:

1. The set $\mathcal{G} = \{\text{CNOT}, \text{H}, \text{T}\}$ [23]
2. The set $\mathcal{G} = \{\text{CNOT}, \text{H}, \text{S}, \text{Toffoli}\}$ [24]

The Solovay-Kitaev Theorem [25, 26] establishes that gates from a universal gate set approximate any unitary transformation to an arbitrary accuracy $\varepsilon$ with the efficiency polylogarithmic in $\frac{1}{\varepsilon}$.

### 2.4 Probabilistic Nature of Quantum Algorithms

The nature of the quantum world dictates that quantum computers are probabilistic devices and can be viewed as a generalization of a probabilistic Turing machine. It is hardly surprising that quantum algorithms exhibit their probabilistic nature by producing a solution with some probability. Suppose we have an algorithm which succeeds with probability $\frac{1}{2} + \delta$ for some fixed constant $\delta$. Then the probability of failure for this algorithm is $\frac{1}{2} - \delta$. 
The algorithm is run $k$ times and we take the majority result. Then the probability that the algorithm fails is given by

$$
Pr = \sum_{l=0}^{\left\lfloor \frac{k}{2} \right\rfloor} \binom{k}{l} \left( \frac{1}{2} + \delta \right)^l \left( \frac{1}{2} - \delta \right)^{k-l}
$$

(2.62)

where $l$ is the number of times the algorithm returns the correct answer.

For $l = \left\lfloor \frac{k}{2} \right\rfloor$ we have

$$
\left( \frac{1}{2} + \delta \right)^{\left\lfloor \frac{k}{2} \right\rfloor} \left( \frac{1}{2} - \delta \right)^{k-\left\lfloor \frac{k}{2} \right\rfloor} = \left( \frac{1 + 2\delta}{2} \right)^{\left\lfloor \frac{k}{2} \right\rfloor} \left( \frac{1 - 2\delta}{2} \right)^{\left\lceil \frac{k}{2} \right\rceil}
$$

(2.63)

\leq \left( \frac{1 - 4\delta^2}{4} \right)^{\frac{k}{2}}

= \left( 1 - 4\delta^2 \right)^{\frac{k}{2}}

\leq \frac{2^k}{2^k}. \tag{2.64}

Since Eq (2.62) contains at most $2^k$ terms $l = \left\lfloor \frac{k}{2} \right\rfloor$, the failure probability is bounded as follows:

$$
Pr \leq 2^k \left[ \frac{1 - 4\delta^2}{2^k} \right]^{\frac{k}{2}} = \left( 1 - 4\delta^2 \right)^{\frac{k}{2}}. \tag{2.65}
$$

Application of

$$
1 - x \leq e^{-x}
$$

(2.65)

produces

$$
\left( 1 - 4\delta^2 \right)^{\frac{k}{2}} \leq \left( e^{-4\delta^2} \right)^{\frac{k}{2}} = e^{-2\delta^2k}
$$

(2.66)

and we obtain a Chernoff bound

$$
Pr \leq e^{-2\delta^2k}. \tag{2.67}
$$

Therefore, the algorithm succeeds with probability exponentially close to 1 in the number of trials.
To illustrate the point convincingly, suppose the algorithms fails with probability $\frac{1}{4}$, i.e., $\delta = \frac{1}{4}$. The approximate Chernoff bounds corresponding to an increasing number of algorithm repetitions are given in Table 2.2.

Table 2.2: The Chernoff bounds for $\delta = \frac{1}{4}$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$e^{-2\delta^2 k}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.286</td>
</tr>
<tr>
<td>40</td>
<td>0.007</td>
</tr>
<tr>
<td>100</td>
<td>$3.73 \times 10^{-6}$</td>
</tr>
<tr>
<td>400</td>
<td>$1.93 \times 10^{-22}$</td>
</tr>
<tr>
<td>1000</td>
<td>$5.17 \times 10^{-55}$</td>
</tr>
</tbody>
</table>

When the probability drops below $10^{-20}$, a failure of the computer itself is more likely than that of an algorithm. For 1000 runs, you are more likely to be hit by an asteroid while reading this sentence than to get a wrong answer from the algorithm!
CHAPTER 3
SHOR’S FACTORIZATION ALGORITHM

The existence of a unique decomposition of any integer \( N > 1 \) into a product of primes was formalized by Euclid around 300 BC in Propositions 30 and 32 of his *Elements* [18]. The first complete proof was provided in 1801 by Carl Friedrich Gauss in his *Disquisitiones Arithmeticae*, where he remarked [19]:

"The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated."

Almost two centuries later Peter Shor discovered a quantum algorithm that factors an integer \( N \) with high probability in

\[
O(n^2 \log_2 n \log_2 \log_2 n)
\]  

steps where \( n \) is the number of bits needed to represent \( N \), an exponential speedup over the best-known classical algorithm.

3.1 Reduction of Factorization to Order Finding

We may assume that an integer \( N \) we wish to factor is odd, as factors of 2 can be easily removed. Moreover, since there exist efficient classical tests for prime powers [30], we assume that \( N \) is an odd non-prime power integer. Miller [42] showed that factorization reduces to order finding.
Choose a random integer $a$ such that $1 < a < N$. The order of $a$ is an integer $r$ such that

$$a^r \equiv 1 \mod N$$

(3.2)

and it is equal to the period of a function defined by

$$f_{a,N}(x) = a^x \mod N.$$  

(3.3)

Use Euclid’s algorithm to find the $\gcd(a, N)$. If $a$ is not coprime to $N$, then $\gcd(a, N)$ is a non-trivial factor of $N$. If $a$ turns out to be coprime to $N$, the order $r$ of $a$ is even with $Pr \geq \frac{1}{2}$. For an even $r$,

$$N \mid \left( a^{r/2} - 1 \right) \left( a^{r/2} + 1 \right).$$

(3.4)

The $\gcd(a^{r/2} - 1, N)$ is a non-trivial factor of $N$ with $Pr \geq \frac{1}{2}$.

Furthermore, the order-finding problem can be reduced to sampling fractions $\frac{j}{r}$ with an integer $\lambda$ chosen uniformly at random from $\{1, \ldots, r - 1\}$. It is not even necessary to determine the fraction $\frac{j}{r}$ exactly; by the theory of continued fractions, all that is required is an estimate $\frac{j}{2n}$ such that

$$\left| \frac{j}{2n} - \frac{\lambda}{r} \right| \leq \frac{1}{2r^2}.$$  

(3.5)

### 3.2 The Quantum Part: Order Finding

#### 3.2.1 The Main Ingredient: Quantum Fourier Transform

Let $G = \{g_1, g_2, \ldots, g_n\}$ be an abelian group with irreducible characters $\{\chi_1, \chi_2, \ldots, \chi_n\}$. The functions $f : G \rightarrow \mathbb{C}$ form a complex vector space $V$ over $\mathbb{C}$ with addition and scalar multiplication
defined by

\[(f + h)(g) = f(g) + h(g)\]

\[(\lambda f)(g) = \lambda f(g)\] (3.6)

for all \(g \in G\), and the standard inner product defined by

\[\langle f | h \rangle = \sum_{k=1}^{n} \overline{f(g_k)}h(g_k)\] (3.7)

The functions

\[B_i = \frac{1}{\sqrt{n}} \chi_i\] (3.8)

form an orthonormal basis of \(V\). Then any function \(f \in V\) can be written as

\[f = \alpha_1 B_1 + \alpha_2 B_2 + \ldots + \alpha_n B_n.\] (3.9)

The coefficients \(\alpha_1, \ldots, \alpha_n \in \mathbb{C}\) are the Fourier coefficients of \(f\).

**Definition 3.2.1.** The function \(\hat{f} \in V\) given by

\[\hat{f}(g_i) = \alpha_i\] (3.10)

is the discrete Fourier transform of \(f \in V\).

Since \(\alpha_i = \langle B_i | f \rangle\),

\[\hat{f}(g_i) = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \overline{\chi_i(g_k)}f(g_k)\] (3.11)

An orthonormal basis of a finite quantum system \(Q\) capable of representing elements of a group \(G\) is the set \(\{|g\rangle : g \in G\}\). Then a mapping \(f : G \to \mathbb{C}\) with \(f(g_i) = \alpha_i\) and \(\|f\| = 1\) defines a general state of \(Q\)

\[|\psi\rangle = \alpha_1 |g_1\rangle + \alpha_2 |g_2\rangle + \ldots + \alpha_n |g_n\rangle\] (3.12)
**Definition 3.2.2.** The Quantum Fourier Transform ($QFT$) is the operation

$$\sum_{i=1}^{n} f(g_i) |g_i\rangle \longrightarrow \sum_{i=1}^{n} \hat{f}(g_i) |g_i\rangle .$$  

(3.13)

The action of the QFT on the basis of $Q$ is

$$|g_i\rangle \longrightarrow \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_k(g_i) |g_k\rangle$$  

(3.14)

with the corresponding matrix

$$\frac{1}{\sqrt{n}} \begin{pmatrix} \chi_1(g_1) & \cdots & \chi_1(g_n) \\ \vdots & \ddots & \vdots \\ \chi_n(g_1) & \cdots & \chi_n(g_n) \end{pmatrix}$$  

(3.15)

**Definition 3.2.3.** The Inverse Quantum Fourier Transform ($QFT^\dagger$) is defined by

$$|g_i\rangle \longrightarrow \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_k(g_i) |g_k\rangle$$  

(3.16)

The characters of a cyclic group $\mathbb{Z}_{2^n}$ are

$$\chi_y(x) = e^{2\pi i \frac{x y}{2^n}}$$  

(3.17)

where $x, y$ are coset representatives. Then the $QFT$ over $\mathbb{Z}_{2^n}$ is the operation

$$|x\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{-2\pi i \frac{x y}{2^n}} |y\rangle .$$  

(3.18)

Since in $\mathbb{Z}_{2^n}$

$$\chi_y(x) = \chi_x(y) ,$$  

(3.19)
the inverse $QFT$ is given by

$$
|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy}{n}} |y\rangle.
$$

(3.20)

A group element

$$
x = x_n 2^{n-1} + x_{n-1} 2^{n-2} + \ldots + x_2 2 + x_1
$$

(3.21)

where $x_i \in \{0, 1\}$, is represented in a quantum system using $n$ qubits as

$$
|x\rangle = |x_n x_{n-1} \ldots x_1\rangle.
$$

(3.22)

The inverse $QFT$ can be decomposed as

$$
QFT^\dagger |x\rangle = \frac{1}{\sqrt{2^n}} \left( |0\rangle + e^{2\pi i (0 x_n)} |1\rangle \right) \otimes \ldots \otimes \left( |0\rangle + e^{2\pi i (0 x_1 x_2 \ldots x_n)} |1\rangle \right)
$$

(3.23)

and thus can be implemented by Hadamard and controlled discrete phase gates, as shown in Figure 3.1.
The QFT over $\mathbb{Z}_2^n$ can be accomplished with time complexity $O(n^2)$, whereas its best classical counterpart, the fast Fourier transform, requires time $O(n2^n)$.

3.2.2 Quantum Algorithm for Order Finding

We have collected all the tools required to present the summary of the heart of Shor’s algorithm. The corresponding quantum circuit is displayed in Figure 3.2.

![Quantum Circuit for Period Finding](image)
1. Initialize a quantum computer in a state

\[ |\psi_0\rangle = |0^\otimes m\rangle |0^\otimes n\rangle \quad (3.24) \]

where

\[ N^2 \leq 2^m < 2N^2, \quad n = \lceil \log_2 N \rceil \]

2. Prepare a superposition

\[ |\psi_1\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle |0\rangle \quad (3.25) \]

by applying \( m \) Hadamard transforms to the top register.

3. Choose an integer \( a \) such that \( 1 < a < N \) and \( \gcd(a, N) = 1 \). Apply a unitary \( U_f \) that computes

\[ f_{a,N}(x) = a^x \mod N, \quad (3.26) \]

a function with period \( r \) to obtain

\[ |\psi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle |a^x \mod N\rangle \quad (3.27) \]

\[ = \frac{1}{\sqrt{2^m}} \sum_{l=0}^{r-1} \sum_{k=0}^{s_l} |kr + l\rangle |a^l \mod N\rangle \quad (3.28) \]

where \( s_l \) is the greatest integer such that

\[ s_l r + l < 2^m \quad (3.29) \]

4. Apply the QFT over \( \mathbb{Z}_{2^m} \) to obtain

\[ |\psi_3\rangle = \frac{1}{2^m} \sum_{l=0}^{r-1} \sum_{k=0}^{s_l} \sum_{p=0}^{2^m-1} e^{-2\pi i \frac{p(kr+l)}{2^m}} |p\rangle |a^l \mod N\rangle \quad (3.30) \]

5. Measure \( |\psi_3\rangle \) to get some \( p \in \mathbb{Z}_{2^m} \).
6. Use Euclid’s algorithm to find the convergents $\frac{p_i}{k_i}$ of the continuous fraction expansion of $\frac{p}{2^m}$. A $k_i < N$ yields the period $r$ or a factor of $r$.

### 3.3 Shor’s Algorithm Applied: An Illustration

To demonstrate important features of Shor’s algorithm, let’s boldly factor $N = 21$. First, the sizes of the top and bottom registers must be determined. The top register must contain $m$ qubits such that

$$N^2 \leq 2^m < 2N^2$$

(3.31)

and for $N = 21$, $m = 9$. There must be at least $n = \lceil \log_2 N \rceil = 5$ qubits in the bottom register.

We now must choose an integer $a$ such that $1 < a < 21$ and $\gcd(a, 21) = 1$. Suppose we pick $a = 2$ and initialize the quantum computer in the state

$$|\psi_0\rangle = |0^{\otimes 9} \rangle |0^\otimes 5\rangle$$

(3.32)

The nine Hadamard gates applied in parallel to the top register

$$H |0^{\otimes 9}\rangle = \frac{1}{\sqrt{2^9}} \sum_{x=0}^{511} |x\rangle$$

(3.33)

put the system in the state

$$|\psi_1\rangle = \frac{1}{\sqrt{512}} \sum_{x=0}^{511} |x\rangle |0\rangle$$

(3.34)

to which we apply the unitary $U_f$ defined by

$$U_f (|x\rangle |y\rangle) = |x\rangle |y \oplus f_{2,21}(x)\rangle = |x\rangle |2^x \mod 21\rangle$$

(3.35)

since

$$y = |0\rangle$$

(3.36)
to produce the state

\[
| \psi_2 \rangle = \frac{1}{\sqrt{512}} \sum_{x=0}^{511} |x \rangle |2^{x \mod 21}\rangle
\]

\[
= \frac{1}{\sqrt{512}} [ |0 \rangle |1\rangle + |1 \rangle |2\rangle + |2 \rangle |4\rangle + |3 \rangle |8\rangle + |4 \rangle |16\rangle + |5 \rangle |11\rangle + \\
|6 \rangle |1\rangle + |7 \rangle |2\rangle + |8 \rangle |4\rangle + |9 \rangle |8\rangle + |10 \rangle |16\rangle + |11 \rangle |11\rangle + \\
|12 \rangle |1\rangle + |13 \rangle |2\rangle + |14 \rangle |4\rangle + \cdots + |510 \rangle |1\rangle + |511 \rangle |2\rangle ].
\]

(3.37)

The state of each register at this point in the circuit is outlined in Table 3.1.

<table>
<thead>
<tr>
<th>Bottom Register</th>
<th>Top Register</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0\rangle +</td>
</tr>
<tr>
<td></td>
<td>1\rangle</td>
</tr>
<tr>
<td></td>
<td>2\rangle</td>
</tr>
<tr>
<td></td>
<td>4\rangle</td>
</tr>
<tr>
<td></td>
<td>8\rangle</td>
</tr>
<tr>
<td></td>
<td>16\rangle</td>
</tr>
</tbody>
</table>

The measurement of the bottom register will now reveal one of \{1, 2, 4, 8, 16, 11\} with equal probability. In fact, the probability of obtaining at least one value from this set is approximately 0.78. If the measurement results in 2, then the state of the system becomes

\[
| \psi_3 \rangle = \frac{1}{\sqrt{86}} (|1\rangle + |7\rangle + |13\rangle + \cdots + |511\rangle) |2\rangle
\]

\[
= \left( \frac{1}{\sqrt{86}} \sum_{k=0}^{85} |6k + 1\rangle \right) |2\rangle.
\]

(3.38)
The subsequent action of the QFT on the top register yields the state

$$|\psi_4\rangle = \text{QFT} \left( \frac{1}{\sqrt{86}} \sum_{k=0}^{85} |6k+1\rangle \right) |2\rangle$$

$$= \frac{1}{\sqrt{512}} \sum_{j=0}^{511} \left( \frac{1}{\sqrt{86}} \sum_{k=0}^{85} e^{-2\pi i \frac{6j k}{512}} \right) e^{-2\pi i \frac{j}{512}} |j\rangle |2\rangle$$

(3.39)

with the probability of a measurement resulting in $j$ given by

$$\text{Pr}(j) = \frac{1}{(512)(86)} \left| \sum_{k=0}^{85} e^{-2\pi i \frac{6j k}{512}} \right|^2$$

(3.40)

The probability plot is displayed in Figure 3.3.

Figure 3.3: Probability Plot

The probability plot shows peaks around $j = 0, 85, 171, 256, 341, 427$, which translates into a high probability of obtaining one of these values as a result of a measurement on the top register.
If \( j = 0 \) is measured, the algorithm must be repeated with the same value of \( a \). If \( j = 85 \) is obtained, the continued fraction expansion of \( \frac{85}{512} \) is used to determine the period \( r \). We have

\[
\frac{85}{512} = \frac{1}{6 + \frac{1}{42 + \frac{1}{2}}} \tag{3.41}
\]

and the set of convergents is

\[
\left\{ \frac{1}{6} \frac{42}{253} \frac{85}{512} \right\}. \tag{3.42}
\]

Since \( r < N \), the denominator of the first convergent is a candidate for the period we seek, and indeed

\[
2^6 \equiv 1 \mod 21. \tag{3.43}
\]

Finally, the factors of 21 are found from

\[
gcd(2^3 + 1, 21) = 3,
\]
\[
gcd(2^3 - 1, 21) = 7. \tag{3.44}
\]

On the other hand, if the measured value is \( j = 171 \) with the relevant convergent of \( \frac{1}{3} \), we obtain only a factor of the period \( r = r_1 r_2 \), namely, \( r_1 = 3 \). Since \( r_2 \) is the order of \( a^{r_1} = 2^3 \), we perform the quantum part of the algorithm with \( a = 8 \) and obtain the missing factor \( r_2 = 2 \). Similarly, the values of \( j = 256 \) and \( j = 341 \) yield factors of the period, requiring that the algorithm is repeated. The value that corresponds to the last peak provides the entire period in the first run.

A detailed analysis shows that the overall success probability of the algorithm for \( a = 2 \) is approximately 0.55.
3.4 Shor’s Algorithm as a Special Case of the Abelian HSP

The quantum part of Shor’s algorithm solves a special case of the abelian HSP with

\[ G = \mathbb{Z} \]
\[ X = \mathbb{Z}_N^\times \]
\[ H = r\mathbb{Z} \]

where \( r \) is the period of the function

\[ f : \mathbb{Z} \to \mathbb{Z}_N^\times \]

defined by

\[ f(x) = a^x \mod N \]

The commutative diagram displayed in Figure 3.4 captures the structure of the problem with the natural epimorphism \( \gamma \) and the monomorphism \( \eta \).

Figure 3.4: Shor’s Algorithm as a Case of HSP

For an algorithm to be physically implementable, the infinite domain of \( f \) must be effectively “restricted”, which is achieved in the modified diagram in Figure 3.5
Figure 3.5: Implementable Shor’s Algorithm as a Case of HSP

\[
\begin{array}{c}
\mathbb{Z} \xrightarrow{f} \mathbb{Z}_N^x \\
\downarrow \mu \\
\mathbb{Z}_R
\end{array}
\]

with an epimorphism $\mu$ onto $\mathbb{Z}_R$, where $R$ is the unique power of 2 such that $N^2 \leq R < 2N^2$.

The transversal

\[
\tau : \mathbb{Z}_R \rightarrow \mathbb{Z}
\]

is defined by

\[
\tau(x \mod R) = x
\]

where $0 \leq x < R$.

The quantum part of Shor’s algorithm produces $j$ and the transversal ensures that for integers $\lambda$ chosen uniformly at random from \{1, ..., $r$ – 1\}

\[
\left| \frac{j}{R} - \frac{\lambda}{r} \right| \leq \frac{1}{2r^2}
\]

which means that $\frac{j}{r}$ is a continued fraction convergent of $\frac{j}{R}$.

(3.46)

(3.47)
CHAPTER 4
HIDDEN SUBGROUP PROBLEM FOR QUATERNIONS

4.1 Tablets From On High: The Story of Quaternions

4.1.1 The Origins

On October 16th, 1843 Sir William R. Hamilton was walking with his wife along the Royal Canal to a meeting of the Royal Irish Academy in Dublin. It had been eight years since he discovered how to treat complex numbers as points in the plane, i.e., as pairs of real numbers \((a, b) = a + ib\). Ever since, Hamilton had been trying to extend the complex numbers to a three-dimensional normed division algebra, a venture doomed from the start; the impossibility of such an algebra was demonstrated by Frobenius in 1877. Unaware of the futility of this approach, Hamilton postulated a triplet \((a, b, c) = a + ib + jc\) with \(i^2 = j^2 = -1\) and \(a, b, c \in \mathbb{R}\). The conjugate of \(a + ib + jc\) is \(a - ib - jc\), and the norm of \((a, b, c)\) is

\[
(a + ib + jc) (a - ib - jc) = (a^2 + b^2 + c^2) - bc (ij + ji).
\] (4.1)

The troublesome term \(bc (ij + ji)\) is removed by sacrificing commutativity and setting

\[
ij = -ji.
\] (4.2)

Yet the sacrifice is not enough.
For an algebra to be closed under multiplication, a product of triplets must produce another triplet, but

\[(a_1 + ib_1 + jc_1)(a_2 + ib_2 + jc_2) = (a_1a_2 - b_1b_2 - c_1c_2) + i(a_1b_2 + b_1a_2) + j(c_1a_2 + a_1c_2) + ij(b_1c_2 - c_1b_2).\] (4.3)

One way to see the impossibility of this feat is to realize that the following must hold in a closed algebra:

\[ij = a + bi + cj\] (4.4)

for \(a, b, c \in \mathbb{R}\). Multiplication of Eq (4.4) by \(i\) yields

\[ai - b + cij + j = 0.\] (4.5)

Substitution of Eq (4.4) into Eq (4.5) produces

\[ai - b + c(a + bi + cj) + j = ai - b + ca + cbi + c^2j + j\]
\[= (ca - b) + (a + cb)i + (c^2 + 1)j\] (4.6)
\[= 0\]

from which a contradiction immediately ensues as

\[c^2 = -1\] (4.7)

and hence \(c \notin \mathbb{R}\).
The breakthrough for Hamilton came on that fateful October day when, in his own words [37]:

*I then and there felt the galvanic circuit of thought close; and the sparks which fell from it were the fundamental equations between i, j, k; exactly such as I have used them ever since.*

A rare act of mathematical vandalism followed: Hamilton pulled out his pocket knife and carved the equations on a side of the bridge. His carving did not survive, but a plaque commemorating the momentous occasion (Figure 4.1) was later placed on the bridge.

![Figure 4.1: Quaternion Plaque on Broom Bridge in Dublin](image)

Hamilton accomplished his extension of complex numbers by leaping from two dimensions straight into four. The quaternion was born as a quadruplet

$$q = a + ib + jc + kd$$  \hspace{1cm} (4.8)

where $i^2 = j^2 = k^2 = -1$ and $a, b, c, d \in \mathbb{R}$.  

The norm of a quaternion $N(q)$ is

$$N(q) = (a + ib + jc + kd) (a - ib - jc - kd) = (a^2 + b^2 + c^2 + d^2)$$

$$-bd (ik + ki) - cd (jk + kj)$$

$$= a^2 + b^2 + c^2 + d^2$$

if

$$ik = -ki$$

and

$$jk = -kj.$$ (4.10)

A complete set of multiplication rules for quaternions is then produced by setting

$$ij = k$$ (4.12)

and the algebra is closed:

$$(a_1 + ib_1 + jc_1 + kd_1) (a_2 + ib_2 + jc_2 + kd_2) = a_1 a_2 + ia_1 b_2 + ja_1 c_2 + ka_1 d_2$$

$$+ ib_1 a_2 + i^2 b_1 b_2 + i j b_1 c_2 + i k b_1 d_2$$

$$+ j c_1 a_2 + j i c_1 b_2 + j^2 c_1 c_2 + j k c_1 d_2$$

$$+ k d_1 a_2 + k i d_1 b_2 + k j d_1 c_2 + k^2 d_1 d_2$$

$$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2)$$ (4.13)

$$+ i (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)$$

$$+ j (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2)$$

$$+ k (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2).$$
Moreover, if $q \neq 0$, then $N(q) = q\bar{q} = \bar{q}q \neq 0$. The inverse of a quaternion is given by

$$q^{-1} = \frac{\bar{q}}{N(q)}$$  \hspace{1cm} (4.14)

Hamilton produced the first example of a noncommutative division ring, on which J.J. Silvester remarked [38]:

_In Quaternions the example has been given of Algebra released from the yoke of the commutative principle of multiplication - an emancipation somewhat akin to Lobachevsky’s of Geometry from Euclid’s noted empirical axiom._

**Proposition 4.1.1.** There are infinitely many square roots of $-1$ in the algebra of Hamilton’s quaternions.

**Proof.** Let $q$ be a pure quaternion, i.e., $q = ia + jb + kc$ with $a, b, c \in \mathbb{R}$ and consider the equation

$$q^2 = -1.$$  \hspace{1cm} (4.15)

We have

$$q^2 = (ia + jb + kc)(ia + jb + kc)$$

$$= -a^2 + ijab + ikac + jiba - b^2 + jkbc + kica + k jcb - c^2$$  \hspace{1cm} (4.16)

$$= - (a^2 + b^2 + c^2) = -1$$

Thus, any pure quaternion of norm 1 is a solution to Eq (4.15), and there are infinitely many such quaternions since they correspond to points on the imaginary 2-sphere. \hfill \Box

41
4.1.2 The Struggle

Hamilton spent much of the remaining twenty-two years of his life on the study of quaternions, publishing 109 papers on the subject. His classic book Lectures on Quaternions appeared in 1853, but his most extensive treatise Elements of Quaternions came from beyond the grave, published in 1866, shortly after Hamilton’s death. He noted the connection between the quaternions and dimensions of time and space [32]:

*Time is said to have only one dimension, and space to have three dimensions...The mathematical quaternion partakes of both these elements; in technical language it may be said to be “time plus space”, or “space plus time”: and in this sense it has, or at least involves a reference to, four dimensions.*

_And how the One of Time, for Space the Three,

Might in the Chain of Symbols girdled be.*

Hamilton was the first to use the terms “scalar” and “vector” in their modern sense when he treated quaternions as having scalar (real) and vector (imaginary) part; he referred to quaternions with zero scalar part as pure quaternions.

Even though many physicists, including James Clerk Maxwell, used quaternions with enthusiasm, they were eventually discarded in favor of the vector algebra promoted by William Gibbs and Olivier Heaviside. One of the reasons was that in most physical applications only the imaginary part of the quaternions was required, so they came to be viewed as unnecessarily complicated. In essence, the vector algebraists simply extracted the vector part of the quaternions, discarding the scalar part, and developed a more consistent notation. But the drawbacks may have outweighed the benefits. It has been argued that if quaternions “had been used in the correct way from early on, they would have pre-empted many later physical developments that came about much more tortuously” [28].

42
A comment made by Bertrand Russell on Plato’s *Theory of Ideas* [29] comes to mind:

*Any attempt to divide the world into portions, of which one is more ’real’ than the other, is doomed to failure.*

The heated controversy over the usefulness of quaternions continued for several generations after Hamilton’s death.

4.1.3 The Revival

The impact of quaternions on the development of mathematical thought is undeniable: much of the work in the theory of algebras descended from Hamilton’s discovery. That quaternions arise naturally in standard quantum mechanics when time reversals are considered was first noted by Dyson [31] in 1962. Since then, other physicists have formulated quaternionic generalizations of the postulates of quantum mechanics, quantum field theory, and gravitational theory.

Advantages of quaternionic forms have been exploited for attitude control in aeronautics and astronautics [34]. Most recently, quaternions have found extensive applications in the fields of 3D computer graphics, animations, and virtual reality; and it all began with a seminal 1985 paper by Shoemake [39].

The Euler-angle method for implementing 3D rotations is susceptible to Gimbal lock, where the order of rotations causes the failure of rotation to appear as expected. Quaternions provide a solution to the problem, allowing the programmer to rotate an object through an arbitrary rotation axis and angle instead of a series of successive rotations. The errors accumulating due to matrix multiplication are avoided, as quaternions representing the axii of rotations are multiplied instead. Moreover, quaternions can be interpolated, thus producing smooth and predictable rotation effects.
4.2 The Group $Q_4$

The generalized quaternion group of order $2^n$, $n \geq 3$, is given by the presentation

$$Q_{2^n} = \langle x, y | x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, y^{-1}xy = x^{-1} \rangle$$

(4.17)

For $n = 2$,

$$Q_4 \cong \mathbb{Z}_4 = \langle x, y | x^2 = 1, x = y^2 \rangle = \langle x | x^4 = 1 \rangle$$

(4.18)

The only subgroups of $\mathbb{Z}_4$ are

$$
\begin{align*}
H_1 &= \{0\} = \langle 4 \rangle \\
H_2 &= \{0, 2\} = \langle 2 \rangle \\
H_3 &= \{0, 1, 2, 3\} = \langle 1 \rangle
\end{align*}
$$

Since a periodic function $f$ with period $r$ on a cyclic group $\langle x \rangle$ hides a subgroup $\langle x^r \rangle$, this case is treated as a special case of period finding, a pivotal part of Shor’s algorithm.

Let $G = \mathbb{Z}_4$, and suppose the black-box function $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ is such that $f(x) = f(x + r)$ for all $x \in \mathbb{Z}_4$. The algorithm is implemented by the circuit in Figure 4.2.

Figure 4.2: Quantum Circuit for Period Finding over $Q_4$
The Hadamard gate puts the qubits in the top register into an equally-weighted superposition:

\[
\frac{1}{\sqrt{2^2}} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2} (|0\rangle + |1\rangle + |2\rangle + |3\rangle).
\] (4.19)

Application of the unitary transformation \( U_f \) produces the state

\[
|\psi_1\rangle = U_f \frac{1}{2} \sum_{x \in \mathbb{Z}_4} |x\rangle |0\rangle = \frac{1}{2} \sum_{x \in \mathbb{Z}_4} |x, f(x)\rangle = \frac{1}{2} (|0, f(0)\rangle + \ldots + |3, f(3)\rangle).
\] (4.20)

The \( QFT \)

\[
|x\rangle \mapsto \frac{1}{2} \sum_{y=0}^{3} e^{2\pi ixy/4} |y\rangle
\] (4.21)

applied to the top register results in the state

\[
|\psi_2\rangle = \frac{1}{4} \sum_{x,y} e^{2\pi ixy/4} |y, f(x)\rangle
\]

\[
= \frac{1}{4} |0\rangle \otimes [|f(0)\rangle + |f(1)\rangle + |f(2)\rangle + |f(3)\rangle]
+ \frac{1}{4} |1\rangle \otimes [e^{2\pi i/4} |f(0)\rangle + e^{2\pi i2/4} |f(1)\rangle + e^{2\pi i3/4} |f(2)\rangle + e^{2\pi i3/4} |f(3)\rangle]
+ \frac{1}{4} |2\rangle \otimes [e^{2\pi i/4} |f(0)\rangle + e^{2\pi i4/4} |f(1)\rangle + e^{2\pi i6/4} |f(2)\rangle + e^{2\pi i6/4} |f(3)\rangle]
+ \frac{1}{4} |3\rangle \otimes [e^{2\pi i3/4} |f(0)\rangle + e^{2\pi i6/4} |f(1)\rangle + e^{2\pi i9/4} |f(2)\rangle + e^{2\pi i9/4} |f(3)\rangle).
\] (4.22)

If \( r = 2 \), the hidden subgroup is \( H_2 = \langle 2 \rangle \), and \( f(0) = f(2) = g_1, f(1) = f(3) = g_2, g_1 \neq g_2 \).
Hence, the state $|\psi_2\rangle$ becomes

$$|\psi_2\rangle = \frac{1}{4} \sum_{x,y} e^{2\pi ixy/4} |y, f(x)\rangle$$

$$= \frac{1}{2} (|0\rangle \otimes [|g_1\rangle + |g_2\rangle]$$
$$+ \frac{1}{4} |1\rangle \otimes [|g_1\rangle (1 + e^{\pi i}) + |g_2\rangle (e^{\pi i/2} + e^{3\pi i/2})]$$
$$+ \frac{1}{4} |2\rangle \otimes [|g_1\rangle (1 + e^{2\pi i}) + |g_2\rangle (e^{\pi i} + e^{3\pi i})]$$
$$+ \frac{1}{4} |3\rangle \otimes [|g_1\rangle (1 + e^{3\pi i}) + |g_2\rangle (e^{\pi i/2} + e^{9\pi i/2})]$$

and reduces to

$$|\psi_2\rangle = \frac{1}{2} (|0, g_1\rangle + |0, g_2\rangle + |2, g_1\rangle - |2, g_2\rangle).$$

Measurement of the top register now yields, with probability $\frac{1}{2}$, either 0 or 2. If 0 is measured, the algorithm must be repeated.

### 4.3 The Group $Q_8$

#### 4.3.1 Group Presentation

The group $Q_8$, usually referred to as the quaternions, is given by

$$Q_8 = \langle x, y | x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle.$$  \hspace{1cm} (4.25)

Following Hamilton’s notation, the group is often written as

$$Q_8 = \{-1, i, j, k | i^2 = j^2 = k^2 = ijk = -1 \}$$  \hspace{1cm} (4.26)

However, it was Arthur Cayley who first observed that the quaternions form a group, so it is fitting to display its full Cayley table.
Table 4.1: Cayley Table for $Q_8$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>-1</th>
<th>i</th>
<th>-i</th>
<th>j</th>
<th>-j</th>
<th>k</th>
<th>-k</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>i</td>
<td>-i</td>
<td>j</td>
<td>-j</td>
<td>k</td>
<td>-k</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>-i</td>
<td>i</td>
<td>j</td>
<td>-j</td>
<td>k</td>
<td>-k</td>
</tr>
<tr>
<td>i</td>
<td>i</td>
<td>-i</td>
<td>-1</td>
<td>1</td>
<td>k</td>
<td>-k</td>
<td>-j</td>
<td>j</td>
</tr>
<tr>
<td>-i</td>
<td>-i</td>
<td>i</td>
<td>1</td>
<td>-1</td>
<td>k</td>
<td>j</td>
<td>-j</td>
<td></td>
</tr>
<tr>
<td>j</td>
<td>j</td>
<td>-j</td>
<td>-k</td>
<td>k</td>
<td>-1</td>
<td>1</td>
<td>i</td>
<td>-i</td>
</tr>
<tr>
<td>-j</td>
<td>-j</td>
<td>j</td>
<td>k</td>
<td>-k</td>
<td>1</td>
<td>-1</td>
<td>-i</td>
<td>i</td>
</tr>
<tr>
<td>k</td>
<td>k</td>
<td>-k</td>
<td>j</td>
<td>-i</td>
<td>-i</td>
<td>-1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>-k</td>
<td>-k</td>
<td>k</td>
<td>-j</td>
<td>j</td>
<td>i</td>
<td>-i</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>

Let $q$ be a quaternion given by

$$q = \alpha + j\beta$$  \hspace{1cm} (4.27)

where $\alpha, \beta \in \mathbb{C}$.

A matrix representation of $q$ in $\mathbb{C}^{2 \times 2}$ is given by

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}.$$  \hspace{1cm} (4.28)

Then the group elements are represented in terms of matrices as follows:

$$i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = ij \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$  \hspace{1cm} (4.29)
A quaternion $q = a + ib + jc + kd$, $a, b, c, d \in \mathbb{R}$ can be represented by the following matrix in $\mathbb{R}^{4 \times 4}$:

$$
\begin{pmatrix}
  a & -b & -c & -d \\
  b & a & -d & c \\
  c & d & a & -b \\
  d & -c & b & a
\end{pmatrix}
$$

(4.30)

4.3.2 Subgroup Classification

**Theorem 4.3.1.** The only nontrivial proper subgroups of $Q_8$ are

$$
H_1 = \{1, -1\} = \langle -1 \rangle \\
H_2 = \{1, -1, i, -i\} = \langle i \rangle \\
H_3 = \{1, -1, j, -j\} = \langle j \rangle \\
H_4 = \{1, -1, k, -k\} = \langle k \rangle
$$

**Proof.** Suppose a subgroup of $Q_8$ contains $i$. Then it must include $-i$, since $i^{-1} = -i$. Similarly, any subgroup of $Q_8$ that contains $j$ (or $k$) must include $-j$ (or $-k$). Moreover, if a subgroup contains $\pm i$, it must include $-1 = (\pm i)^2$. Similarly, any subgroup that contains $\pm j$ (or $\pm k$) must contain $-1 = (\pm j)^2 = (\pm k)^2$. Finally, if a subgroup contains any two of $i, j, k$, it must be $Q_8$ itself since $ij = k$, $jk = i$ and $ik = -j$. 

\[\square\]

**Lemma 4.3.2.** All subgroups of $Q_8$ are normal.

**Proof.** The group $Q_8$ has a unique element of order 2 and it generates $H_1 = \langle -1 \rangle$. Then every subgroup of $Q_8$, except for $\{1\}$, possess $H_1$ as its subgroup, and since $Q_8/H_1 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is abelian, every subgroup is normal.

\[\square\]
4.3.3 Group Construction

Consider a homomorphism $\varphi : \mathbb{Z}_4 \rightarrow \text{Aut}(\mathbb{Z}_4)$, completely determined by the image of the generator 1 of $\mathbb{Z}_4$. An automorphism $\theta$ of $\mathbb{Z}_4$ maps 1 to a generator of $\mathbb{Z}_4$ so we have either $\theta(1) = 1$ or $\theta(1) = -1$. Therefore, $\text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$. If a homomorphism $\varphi : \mathbb{Z}_4 \rightarrow \text{Aut}(\mathbb{Z}_4)$ sends 1 to the identity automorphism, we have a direct product $\mathbb{Z}_4 \times \mathbb{Z}_4$, an abelian group. On the other hand, a mapping to the automorphism $\theta(m) = -m$ results in a non-abelian semi-direct product $\mathbb{Z}_4 \rtimes \varphi \mathbb{Z}_4$ with the group law

$$(a,b)(c,d) = (a + \varphi_b(c), b + d)$$  \hfill (4.32)

where $\varphi_y(z) = z$ for $y$ even, and $\varphi_y(z) = -z$ for $y$ odd so that

$$(a,b)(c,d) = \left(a + (-1)^b c, b + d\right)$$  \hfill (4.33)

**Theorem 4.3.3.** Let $K = \mathbb{Z}_4 \rtimes \mathbb{Z}_4$ with the group operation given by

$$(a,b)(c,d) = \left(a + (-1)^b c, b + d\right)$$  \hfill (4.34)

Then

$$\frac{K}{\langle (2,2) \rangle} \cong Q_8$$  \hfill (4.35)

**Proof.** Let $N = \langle (2,2) \rangle$. Application of the group operation to $(2,2)$ yields

$$(2,2)^2 = (2,2)(2,2) = \left(2 + (-1)^2 2, 2 + 2\right) = (4,4) = (0,0),$$  \hfill (4.36)

i.e., the order of $(2,2)$ in $K$ is 2, and $|N| = 2$. Thus,

Moreover, \((2, 2) \in Z(K)\) since
\[
(2, 2) (c, d) = \left( 2 + (-1)^2 c, 2 + d \right) = (2 + c, 2 + d)
\] (4.37)

and
\[
(c, d) (2, 2) = \left( c + (-1)^d 2, d + 2 \right)
= \left( (-1)^d 2 + c, 2 + d \right) = (2 + c, 2 + d).
\] (4.38)

Therefore, \(N \triangleleft K\), and we can form the quotient group \(\frac{K}{N}\).

Let \(\phi : K \to Q_8\) be defined by
\[
\phi(a, b) = i^a j^b.
\] (4.39)

From
\[
\phi((a, b) (c, d)) = \phi \left( a + (-1)^b c, b + d \right) = i^{a+(-1)^b c} j^{b+d}
\] (4.40)

and
\[
\phi(a, b) \phi(c, d) = \left( i^a j^b \right) \left( i^c j^d \right) = i^a j^b \left( i^c j^{-b} \right) j^d = i^a \left( j^b i^c j^{-b} \right) \left( j^b j^d \right)
= i^a \left( j^b i j^{-b} \right) j^{b+d} = i^a i^c j^{b+d} = i^{a+(-1)^b c} j^{b+d}
\] (4.41)

it follows that \(\phi\) is a homomorphism.

Moreover, since \(\phi(1, 0) = i\) and \(\phi(0, 1) = j\), the image of \(\phi\) is the entire group \(Q_8\), and \(\phi\) is an epimorphism. Also, \((2, 2) \in \ker \phi\) since \(\phi(2, 2) = i^2 j^2 = 1\).
Then there is an epimorphism

$$\frac{\mathbb{Z}_4 \rtimes \mathbb{Z}_4}{\langle (2, 2) \rangle} \to \mathbb{Q}_8$$  \hspace{1cm} (4.42)

which must be an isomorphism since

$$\frac{|\mathbb{Z}_4 \rtimes \mathbb{Z}_4|}{|\langle (2, 2) \rangle|} = |\mathbb{Q}_8|.$$  \hspace{1cm} (4.43)

The mappings

$$-1 \mapsto x^2$$

$$i \mapsto x$$

$$j \mapsto y$$

$$k \mapsto xy$$

produce a Cayley table (Table 4.2) based on the presentation given in Eq (4.25).

Table 4.2: Multiplication Table for $\mathbb{Q}_8$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>$x$</th>
<th>$x^2$</th>
<th>$x^3$</th>
<th>$y$</th>
<th>$xy$</th>
<th>$x^2y$</th>
<th>$x^3y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$x$</td>
<td>$x^2$</td>
<td>$x^3$</td>
<td>$y$</td>
<td>$xy$</td>
<td>$x^2y$</td>
<td>$x^3y$</td>
</tr>
<tr>
<td>$x$</td>
<td>$x$</td>
<td>$x^2$</td>
<td>$x^3$</td>
<td>1</td>
<td>$xy$</td>
<td>$x^2y$</td>
<td>$x^3y$</td>
<td>$y$</td>
</tr>
<tr>
<td>$x^2$</td>
<td>$x^2$</td>
<td>$x^3$</td>
<td>1</td>
<td>$x$</td>
<td>$x^2y$</td>
<td>$x^3y$</td>
<td>$y$</td>
<td>$xy$</td>
</tr>
<tr>
<td>$x^3$</td>
<td>$x^3$</td>
<td>1</td>
<td>$x$</td>
<td>$x^2$</td>
<td>$x^3y$</td>
<td>$y$</td>
<td>$xy$</td>
<td>$x^2y$</td>
</tr>
<tr>
<td>$y$</td>
<td>$y$</td>
<td>$x^3y$</td>
<td>$x^2y$</td>
<td>$xy$</td>
<td>$x^2$</td>
<td>$x$</td>
<td>1</td>
<td>$x^3$</td>
</tr>
<tr>
<td>$xy$</td>
<td>$xy$</td>
<td>$y$</td>
<td>$x^3y$</td>
<td>$x^2y$</td>
<td>$x^3$</td>
<td>$x^2$</td>
<td>$x$</td>
<td>1</td>
</tr>
<tr>
<td>$x^2y$</td>
<td>$x^2y$</td>
<td>$xy$</td>
<td>$y$</td>
<td>$x^3y$</td>
<td>1</td>
<td>$x^3$</td>
<td>$x^2$</td>
<td>$x$</td>
</tr>
<tr>
<td>$x^3y$</td>
<td>$x^3y$</td>
<td>$x^2y$</td>
<td>$xy$</td>
<td>$y$</td>
<td>$x$</td>
<td>1</td>
<td>$x^3$</td>
<td>$x^2$</td>
</tr>
</tbody>
</table>
Any element of $Q_8$ can be written in the form $x^ay^b$, with $a \in \mathbb{Z}_4, b \in \mathbb{Z}_2$, so we can treat $Q_8$ as a group consisting of the elements $(a, b) \in \mathbb{Z}_4 \times \mathbb{Z}_2$, with a “twisted” multiplication given by

$$(a, b) (c, d) = \left( a + (-1)^b c + 2bd, b + d \right)$$

(4.45)

where $b, d \in \{0, 1\}$.

Table 4.3: “Twisted” Multiplication

<table>
<thead>
<tr>
<th></th>
<th>$(c,0)$</th>
<th>$(c,1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(a,0)$</td>
<td>$(a+c,0)$</td>
<td>$(a+c,1)$</td>
</tr>
<tr>
<td>$(a,1)$</td>
<td>$(a-c,1)$</td>
<td>$(a-c+2,0)$</td>
</tr>
</tbody>
</table>

4.4 The Generalized Quaternions

4.4.1 Group Presentation and Construction

**Definition 4.4.1.** A finite group is a $p$–group if its order is a power of a prime number $p$.

An example of a $p$–group is the generalized quaternion group of order $2^n$, $n \geq 3$, given by the presentation

$$Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, y^{-1}xy = x^{-1} \rangle$$

(4.46)

Quaternions of norm 1 are referred to as unit quaternions, and they form the group $S^3$, the 3-sphere.

**Theorem 4.4.2.** Every generalized quaternion group is a subgroup of $S^3$.

**Proof.** Let $\omega = e^{\frac{\pi i}{2^{n-2}}}$ and $G$ be the subgroup of $S^3$ generated by $\omega$ and $j$.

We have

$$j^{-1} \omega j = \omega^{-1}$$

(4.47)

$$\omega^{2^{n-2}} = e^{\pi i} = -1 = j^2$$

(4.48)

$$\omega^{2^{n-1}} = 1$$

(4.49)
Therefore, there exists an epimorphism $\phi : Q_{2^n} \to G$. Let $q \in \ker \phi$ such that $q = x^ay^b$ where $a \in \mathbb{Z}_{2^n-1}$ and $b \in \mathbb{Z}_2$. Then
\[
\omega^a \cdot j^b = 1 \tag{4.50}
\]
and so $a = b = 0$. Thus, the kernel is trivial and
\[
Q_{2^n} \cong G. \tag{4.51}
\]

There is a matrix representation for $Q_{2^n}$ over $\mathbb{C}$ which sends
\[
x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{4.52}
\]
where $\omega = e^{\frac{\pi i}{2n-2}}$.

**Theorem 4.4.3.** Let $K = \mathbb{Z}_{2^n-1} \rtimes \mathbb{Z}_4$ with the group operation given by
\[
(a,b)(c,d) = \left(a + (-1)^b c, b + d\right) \tag{4.53}
\]

Then
\[
\frac{K}{\langle(2^{n-2}, 2)\rangle} \cong Q_{2^n}. \tag{4.54}
\]

**Proof.** Let $N = \langle(2^{n-2}, 2)\rangle$. We have
\[
(2^{n-2}, 2)^2 = (2^{n-2}, 2)(2^{n-2}, 2) = \left(2^{n-2} + (-1)^2 2^{n-2}, 2 + 2\right) = (2^{n-1}, 4) = (0, 0) \tag{4.55}
\]
i.e., the order of $(2^{n-2}, 2)$ in $K$ is 2, and $|N| = 2$. 

53
From

\[ |K| = |\mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_4| = |\mathbb{Z}_{2^{n-1}}| |\mathbb{Z}_4| = 2^{n-1} \cdot 4 = 2^n + 1 \quad (4.56) \]

it follows that

\[ \left| \frac{K}{\langle (2^{n-2}, 2) \rangle} \right| = \frac{2^{n+1}}{2} = 2^n = |Q_{2^n}|. \quad (4.57) \]

Also,

\[ (2^{n-2}, 2) (c, d) = \left( 2^{n-2} + (-1)^2 c, 2 + d \right) = (2^{n-2} + c, 2 + d) \quad (4.58) \]

and

\[ (c, d) ( (2^{n-2}, 2) ) = \left( c + (-1)^d 2^{n-2}, d + 2 \right) = \left( (-1)^d 2^{n-2} + c, 2 + d \right) \]

\[ = (2^{n-2} + c, 2 + d) \quad (4.59) \]

since

\[ -2^{n-2} \equiv 2^{n-2} \mod 2^{n-1}. \quad (4.60) \]

Therefore, \( (2^{n-2}, 2) \in Z(K) \) and \( N \triangleleft K \).

Define \( \phi : K \to Q_{2^n} \) by

\[ \phi (a, b) = x^a y^b. \]

From

\[ \phi ((a, b) (c, d)) = \phi \left( a + (-1)^b c, b + d \right) = x^{a+(-1)^b c} y^{b+d} \quad (4.61) \]

and

\[ \phi (a, b) \phi (c, d) = \left( x^a y^b \right) \left( x^c y^d \right) = x^a y^b x^c \left( y^{b+c} y^d \right) = x^a \left( y^b x^c \left( y^{b+c} y^d \right) \right) \]

\[ = x^a \left( y^b x^c \right)^d \left( y^{b+d} \right) = x^a \left( (-1)^b c, y^{b+d} \right) = x^{a+(-1)^b c} y^{b+d} \quad (4.62) \]

we conclude that \( \phi \) is a homomorphism.
Moreover, since $\phi(1, 0) = x$ and $\phi(0, 1) = y$, $\phi$ is an epimorphism.

Also, $(2^{n-2}, 2) \in \ker \phi$ since

$$\phi(2^{n-2}, 2) = x^{2^{n-2}} y^2 = y^4 = 1. \quad (4.63)$$

Then there is an epimorphism

$$\mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_4 \langle (2^{n-2}, 2) \rangle \longrightarrow Q_{2^n} \quad (4.64)$$

that must be an isomorphism since

$$\frac{|\mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_4 \langle (2^{n-2}, 2) \rangle|}{|Q_{2^n}|}. \quad (4.65)$$

\[ \square \]

**Corollary 4.4.4.** Any element of $Q_{2^n}$ can be written uniquely in the form $x^a y^b$, where $a \in \mathbb{Z}_{2^{n-1}}$, $b \in \mathbb{Z}_2$ with multiplication given by

$$(a, b) (c, d) = \left( a + (-1)^b c + 2^{n-2} bd, b + d \right). \quad (4.66)$$

Note that due to the relation $x^{2^{n-2}} = y^2$, it suffices to consider only $b \in \{0, 1\}$.

Hence, the generalized quaternion group can be written as

$$Q_{2^n} = \{(a, b) \mid a \in \mathbb{Z}_{2^{n-1}}, b \in \mathbb{Z}_2\} \quad (4.67)$$

### 4.4.2 Subgroup Structure

**Theorem 4.4.5.** The subgroups of $Q_{2^n}$ are cyclic or generalized quaternion.

**Proof.** It is known that if a finite $p$-group $G$ has only one subgroup of order $p$, then $G$ is cyclic or generalized quaternion. The group $Q_{2^n}$ is a finite $2$-group with a unique subgroup of order 2. Then every non-trivial subgroup of $Q_{2^n}$ has only one subgroup of order 2. Hence, the subgroups
of $Q_{2^n}$ are cyclic or generalized quaternion.

Lemma 4.4.6. For $n \geq 4$, the group $Q_{2^n}$ contains a non-normal subgroup.

Proof. The subgroup group $K = \langle y \rangle$ is not a normal subgroup since for $x \in Q_{2^n}$

$$xyx^{-1} = x^2y$$ (4.68)

and $x^2y \notin K$.

The subgroups are of the forms:

1. $\langle (a,0) \rangle$ with $a = 0$ or $a \mid 2^{n-2}$
2. $\langle (b,1) \rangle$ with $b \in \mathbb{Z}_{2^{n-1}}$.
3. $\langle (a,0), (b,1) \rangle$ with $a \mid 2^{n-2}$ and $b \in \mathbb{Z}_a$.

4.5 Hidden Subgroup Algorithm for Generalized Quaternions

4.5.1 Hidden Subgroup Problem for Generalized Quaternions

The hidden subgroup problem for generalized quaternions (QHSP) is defined as follows.

**Definition 4.5.1 (QHSP).** Given a black-box function $f : Q_{2^n} \rightarrow S$ that maps elements of $Q_{2^n}$ into some finite set $S$ and is known to be constant and distinct on left cosets of a subgroup $H \leq Q_{2^n}$, find a generating set for $H$.

Suppose the hidden subgroup $H$ is of the form $\langle (a,0), (b,1) \rangle$ with $a \mid 2^{n-2}$ and $b \in \mathbb{Z}_a$. Consider the restricted function $\tilde{f} = f|_K$ where $K = \langle (1,0) \rangle \cong \mathbb{Z}_{2^{n-1}}$. Then $\tilde{f}$ hides the subgroup $\tilde{H} = \langle (a,0) \rangle$, and $a$ can be extracted efficiently using Shor's algorithm, since $K$ is abelian. The commutative diagram in Figure 4.3 illustrates the reduction of the QHSP over $Q_{2^n}$ to the QHSP over $Q_{2^n}/\tilde{H}$. 

56
Lemma 4.5.2. The group $\bar{H} = \langle (a, 0) \rangle$ is a normal subgroup of $Q_{2^n}$.

Proof. The inverse of any $(c, d) \in Q_{2^n}$ is given by

\[ (c, d)^{-1} = \left( -(-1)^d c + 2^{n-2}d, d \right) \quad (4.69) \]

since

\[
(c, d) (c, d)^{-1} = (c, d) \left( -(-1)^d c + 2^{n-2}d, d \right) = \left( c + (-1)^d (-(-1)^d c + 2^{n-2}d) + 2^{n-2}dd, 2d \right) = (0, 0). \quad (4.70)
\]

Then for any $(a, 0) \in \bar{H}$

\[
(c, d) (a, 0) (c, d)^{-1} = \left( (-1)^d a, 0 \right) \in \bar{H}. \quad (4.71)
\]

Hence, $\bar{H} \triangleleft Q_{2^n}$.  \hfill \square

Let $\hat{Q} = Q_{2^n} / \bar{H}$ and define a function $\hat{f} : \hat{Q} \to S$ by $\hat{f} \left( g + \bar{H} \right) = f \left( g \right)$ for all $g \in Q_{2^n}$. Then the function $\hat{f}$ hides the subgroup $\hat{H} = H / \bar{H} = \langle (b, 1) \rangle$, and it suffices to consider subgroups of the form $\langle (b, 1) \rangle$. 

57
We have
\[(b, 1)^2 = (b, 1)(b, 1) = (b + (-1)b + 2^{n-2}, 2) = (2^{n-2}, 0).\] (4.72)

Since \((2^{n-2}, 0)\) corresponds to \(j^2 = -1\), the QHSP reduces to finding a hidden \(\sqrt{-1}\), and ultimately to determining \(b\).

4.5.2 Coset Sample Generation Procedure

Let \(|REG_1\rangle, |REG_2\rangle\) denote the top (input) register and the bottom (output) register, respectively. The algorithm starts with a coset sample generation procedure (CSG) that produces single-qubit states of a particular form, with \(b\) encoded in a phase factor. The routine CSG is given by the following sequence.

1. Create the uniform superposition over all elements of \(Q_{2^n}\), i.e., the state
\[|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{(x,y) \in Q_{2^n}} |x, y\rangle.\] (4.73)

2. Query the black-box function \(f\) to obtain the state
\[|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{(x,y) \in Q_{2^n}} |x, y\rangle |f(x, y)\rangle.\] (4.74)

3. Measure \(|REG_2\rangle\) to collapse the state (4.74) to
\[|\psi_2\rangle = \frac{1}{\sqrt{2}} (|x, 0\rangle + |x + b, 1\rangle).\] (4.75)
4. Apply the $QFT^\dagger$ to $|REG_1\rangle$ to produce the state

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{z=0}^{2^n-1} \left( e^{2\pi i \frac{xz}{2^n}} |z, 0\rangle + e^{2\pi i \frac{(x+b)}{2^n}} |z, 1\rangle \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{2\pi i \frac{xz}{2^n}} |z\rangle \otimes \left( |0\rangle + e^{2\pi i \frac{b}{2^n}} |1\rangle \right).$$ (4.76)

5. Measure $|REG_1\rangle$ to obtain the state

$$|\psi_z\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{2\pi i \frac{zb}{2^n}} |1\rangle \right)$$ (4.77)

for some $z$ chosen uniformly at random from $\{0, 1, \ldots, 2^n - 1\}$.

We now exploit the form of $|\psi_z\rangle$ to find the least significant bit of $b$.

**Proposition 4.5.3.** All the bits of $b$ can be determined with $n$ iterations of an algorithm that finds the least significant bit of $b$.

**Proof.** The group $Q_{2^n}$ contains two subgroups isomorphic to $Q_{2^{n-1}}$, namely,

$$G_1 = \{(2a, 0), (2a, 1) \mid a \in \mathbb{Z}_{2^{n-1}} \}$$ (4.78)

$$G_2 = \{(2a, 0), (2a + 1, 1) \mid a \in \mathbb{Z}_{2^{n-1}} \}.$$ (4.79)

If $b$ is even, then $H \leq G_1$, where $H$ is the hidden subgroup. On the other hand, if $b$ is odd, then $H \leq G_2$. Once an algorithm determines the parity of $b$, the hiding function $f$ is restricted to $G_1$ or $G_2$, and the algorithm is called with a modified oracle. The algorithm outputs the least significant bit of $b$ within an appropriate subgroup, and this result corresponds to the second least significant bit of $b$ in $Q_{2^n}$. Therefore, $n$ iterations of the algorithm determine all bits of $b$. 

59
4.5.3 The Kuperberg Sieve

The goal is to prepare the state

\[ |\psi_{2n-1}\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{2\pi i \frac{(2n-1)b}{2^n}} |1\rangle \right) = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{\pi i b} |1\rangle \right) \]

which is subsequently subjected to a measurement in the Hadamard basis

\[ |\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \]

(4.81)

(4.82)

(4.83)

(4.84)

such that application of Hadamard to the state (4.80) yields

\[ H |\psi_{2n-1}\rangle = \left( \frac{1 + (-1)^b}{2} \right) |0\rangle + \left( \frac{1 - (-1)^b}{2} \right) |1\rangle. \]

(4.83)

If \( b \) has even parity, the measurement results in

\[ H \left( \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right) = |0\rangle. \]

(4.84)
If the parity of $b$ is odd, the result is

$$H\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = |1\rangle. \quad (4.85)$$

However, the routine $CSG$ produces the desired state (4.80) with an exponentially small probability of $\frac{1}{2^n}$. The Kuperberg sieve resolves this difficulty by combining states of the form (4.77) to generate states of the same form but with preferred values of $z$.

The Kuperberg sieve is essentially a sequence of $m = \lceil \sqrt{n-1} \rceil$ routines such that the output of routine $j$ is input to routine $j + 1$ for any $j \in \{1, \ldots, m\}$. The input to the first routine is the output of $CSG$, i.e., single-qubit states of the form (4.77), each with a corresponding label $z$ chosen uniformly at random from $\{0, 1, \ldots, 2^n - 1\}$. The output of routine $j$ are qubits such that their labels have $jm$ least significant bits equal to 0 and $n - jm$ bits chosen uniformly at random. Each routine generates qubits whose labels have $m$ additional bits set to 0.

The process of combining the qubits is implemented as follows. Each routine $j$ maintains a batch of qubits, which is initially empty. When a new qubit comes in, the routine compares the $m$ bits in positions $(j-1)m + 1, \ldots, jm$ of its label to the bits in the same label positions in all of the qubits already in its batch. If no qubit already accumulated in the batch has matching label bits, the newly arrived qubit is added to the batch. If there is a match, the new qubit is combined with the matching one.
Proposition 4.5.5. There exists a procedure that with probability \( \frac{1}{2} \) implements the mapping

\[
(z_1, |\psi_{z_1}\rangle) + (z_2, |\psi_{z_2}\rangle) \mapsto (z_1 - z_2, |\psi_{z_1 - z_2}\rangle)
\]  

(4.86)

Proof. Suppose \( CSG \) generates states

\[
|\psi_{z_1}\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{\frac{2\pi i z_1}{2^n}} |1\rangle \right)
\]

\[
|\psi_{z_2}\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{\frac{2\pi i z_2}{2^n}} |1\rangle \right)
\]

(4.87)

with labels \( z_1 \) and \( z_2 \), respectively. The tensor product of these states is given by

\[
|\psi_{z_1, z_2}\rangle = \frac{1}{2} \left( |00\rangle + e^{\frac{2\pi i z_1}{2^n}} |10\rangle + e^{\frac{2\pi i z_2}{2^n}} |01\rangle + e^{\frac{2\pi i (z_1 + z_2)}{2^n}} |11\rangle \right).
\]

(4.88)

Application of a CNOT gate with the first qubit playing the role of a control results in the state

\[
|\psi_{z_1, z_2}\rangle \mapsto \frac{1}{2} \left( |00\rangle + e^{\frac{2\pi i z_1}{2^n}} |11\rangle + e^{\frac{2\pi i z_2}{2^n}} |01\rangle + e^{\frac{2\pi i (z_1 + z_2)}{2^n}} |10\rangle \right)
\]

= \frac{1}{\sqrt{2}} \left[ \left( |0\rangle + e^{\frac{2\pi i (z_1 + z_2)}{2^n}} |1\rangle \right) \otimes |0\rangle \right]

\[
+ \frac{1}{\sqrt{2}} \left[ \left( e^{\frac{2\pi i z_2}{2^n}} |0\rangle + e^{\frac{2\pi i z_1}{2^n}} |1\rangle \right) \otimes |1\rangle \right]
\]

(4.89)

= \frac{1}{\sqrt{2}} \left( |\psi_{z_1 + z_2}, 0\rangle + e^{\frac{2\pi i z_2}{2^n}} |\psi_{z_1 - z_2}, 1\rangle \right).

Measurement of the second qubit yields \( |1\rangle \) with probability \( \frac{1}{2} \), leaving the first qubit in the state \( |\psi_{z_1 - z_2}\rangle \), up to an inconsequential global phase. \( \square \)

The Kuperberg sieve discards the combined qubits of the form \( |\psi_{z_1 + z_2}\rangle \), and by iterating the combination process ensures that the last routine in the sequence outputs the desired state \( |\psi_{2^n - 1}\rangle \). Kuperberg showed [16] that given an input of \( 2^{O(\sqrt{n})} \) qubits, the sieve generates the desired state with high probability.
Quaternions’ potential in the world of quantum computation is just beginning to be explored. Perhaps a quaternionic formulation of quantum mechanics applied to a quantum computational framework could lead to an improvement of existing quantum algorithms or to the emergence of new ones. And if everything three-dimensional is ultimately quaternionic, quaternions could make significant, even profound, contributions in subjects as diverse as cosmology and biology, shedding new light on the unfolding cosmos and the origins of life.

As Hamilton put it [43],

\[
\begin{align*}
\text{If some new truth, O Friend! thy toil discover,} \\
\text{If thine eyes first by some fair form be blest,} \\
\text{Love it for what it is, and as a lover} \\
\text{Gaze, or with joy receive thine honoured guest:} \\
\text{The new-found thought set free, awhile may hover} \\
\text{Gratefully near thee, but it cannot rest.}
\end{align*}
\]
REFERENCES


