Fault-Tolerant Quantum Computing

Arijit Ghosh
Masters Thesis under the supervision of
Prof. Sudebkumar Prasant Pal
Department of Computer Science and Engineering
Indian Institute of Technology
and
Prof. Robert Raussendorf
Department of Physics and Astronomy
The University of British Columbia

CERTIFICATE

This is to certify that the dissertation entitled *"Fault-Tolerant Quantum Computation"*, submitted by Mr. Arijit Ghosh to the Department of Mathematics, Indian Institute of Technology, Kharagpur, in partial fulfillment of the requirements of the degree of *Master of Technology* in *Computer Science and Engineering*, is an authentic record of the work carried out by him under our supervision and guidance.

In my opinion, this work fulfills the requirements for which it has been submitted and has not been submitted to any other Institution for any degree.

Prof. Sudebkumar Prasant Pal

Dr. Robert Raussendorf

Acknowledgements

Arijit Ghosh

Abstract

Quantum Computing is an exciting alternative model to classical computation. In short the theory of quantum computation and quantum information deals with the tasks of computing and information processing that can be accomplished using small systems which follow the fundamental laws of quantum mechanics. The field has received considerable interests after Shor's polynomial time quantum algorithm for factorization of numbers [S97], a problem which still has no polynomial algorithm in the classical model and is strongly believed not to belong to the class **P** of *polynomial time solvable* algorithms, and Grover's quantum search algorithm which finds an element in an unsorted array in $O(\sqrt{n})$ time, a task which cannot be done in better than $O(n)$ time in the classical model, where n is the size of the array. One of the most difficult hurdles in quantum computation and information is decoherence of the quantum mechanical systems which makes the results obtained after processing erroneous. Since the quantum mechanical systems are very small it is very difficult to remove decoherence completely out of the system. Hence the task at hand is to develop schemes that guarantee results of satisfiable quality i. e, fault-tolerance. In this direction Shor proved the fault-tolerance the for the circuit model of quantum computation. Circuit model for quantum computation is analogous to the circuit model of classical computation. Our work here is on fault-tolerance of other quantum computing models like that of quantum cellular automata and adiabatic quantum computing both of which have been shown to be equivalent to circuit model of quantum computing [DA, RR].

As already mentioned implementation is an important problem in Quantum Computation. Which is why it will be very helpful if one can design a scheme that reduces the complexity of the implementation. So the task at hand right now is to design an architecture which is simple, computationally powerful and robust. Physical complexity can be reduced considerably if there are symmetries in the design. Quantum cellular automata (QCA) is computation model where the arrangements of the physical qubits and the gate operation are translation invariant. It has been already shown that one-dimensional QCA [JW95] can simulate any quantum computer. So quantum cellular automata has most of above mentioned qualities except the fact that it is still not

known whether we can develop an fault tolerant scheme to implement quantum cellular automata without losing the topological symmetry of the qubits or the translation invariant gate operations.

Consider a one-dimensional chain of N qubits initialized in the state $|00..0\rangle$ which is applied with the transition function

$$T = (\bigotimes_{i=1}^{N-1} \Lambda(Z)_{i,i+1})(\bigotimes_{i=1}^{N} H_i). \tag{1}$$

That is in each elementary step we first apply first Hadamard gate to each qubits and then conditional Z to each neighboring qubits. And in between each transition operation one may apply transition invariant unitary transformation of the form

$$U_A(\alpha) = \bigotimes_{j=1}^{N} exp(i\frac{\alpha}{2}A_j) \tag{2}$$

where $j = \{X, Y, Z\}$ and j implies the bit at which the gate is applied. It has been shown by Robert in [**?**] that one can implement one-dimensional QCA using these operation. In this thesis I implemented this one-dimensional scheme of QCA using surface codes [Kitaev03]. The physical qubits are arranged in the lattice edges and they satisfy stabilizer operation [NC], i. e they remain unchanged on application of some operations

$$S_X(v) = \bigotimes_{e \in v} X_e, \qquad S_Z(f) = \bigotimes_{e \in f} Z_e \tag{3}$$

where v and f are the sites and the faces of the lattice and e corresponds to the edges of the faces and sites. This is an important property of surface codes which will be helpful in the fault-tolerance. The logical qubits and logical gate operations are encoded in some form in the surface code and physical gate operations respectively. All the operation that will be done on the qubits of the lattice edges will be translation invariant in the physical layer of the lattice. The scheme that we have developed will have both error detection and correction properties.

The paper entitled "Quantum Computation by Adiabatic Evolution" by Farhi et al. [EJSM] is a seminal work in the area of quantum computation. The quantum adiabatic theorem [M76] can be used to develop algorithm to solve the 3-SAT problem, , 2-SAT on a ring and the Grover Problem as shown in [EJSM]. For the 3-SAT problem the running time for the algorithm is not known but for the 2-SAT on a ring problem the running

time is $O(n^3)$, where n is the size of the input. Aharonov et al. in there paper [DA] showed that adiabatic quantum computer is polynomially equivalent to the standard quantum circuit model of computing. This equivalence is an important step which will help in designing new quantum algorithms for problems that till now have no known efficient algorithm in the standard quantum circuit model and also help in constructing fault tolerant quantum computers. Since I was working on the fault-tolerance adiabatic quantum computing and error correcting codes are an important technique used in circuit model to make robust systems hence I started studying the paper named "Error Correcting Codes for Adiabatic Quantum Computation" by Jordan et al. [JFS]. In this paper it was show how addition of a constant energy gap is possible using error correcting codes that protects against $1-$ and $2-$local noises. Stabilizer codes are used to add the constant energy gap to the adiabatic evolution.

Since it has been shown 2-local Hamiltonians can simulate a quantum computer [DA] it is very important to investigate few examples of 2-local Hamiltonians under adiabatic evolution. One very good example is the Ising Model in a transverse magnetic field which solves a very simple problem of finding a n-bit number where all the bits are same. The Ising Hamiltonian is given by the equation

$$H(t) = -t \sum_{i=1}^{N} X_i - (1-t) \sum_{i=1}^{N} Z_i Z_{i+1}, \quad 0 \leq t \leq 1 \tag{4}$$

I have studied the Ising model [SS] in transverse magnetic field and have worked out the details of the diagonalization of the Ising model with using Jordan-Wigner and Bogoliubov transformations [SS] for the cases $n = 2, 3$ and checked the results with the numerical simulations. In addition to the above I numerically plotted the eigenvalues w.r.t time for the Ising model for $n = 4, 5, 6$ qubits. I have plotted the eigenvalues vs time for the encoded Ising model $n = 2, 3$ logical bits case and checked with the eigenvalues obtained from the analytical calculations done previously. I used 4-qubit encoding from [JFS] that protects against 1-local noises. For this work I had to learn *Canonical Commutation Relations* (*CCRs*) for Fermions, consequences of the fremionic CCRs, diagonalization of Fermi quadratic Hamiltonian and Jordan-Wigner and Bogoliubov transformations. I followed [SS] and [Nielsen] for this part of the work.

I worked on JFS [JFS] encoding for adiabatic quantum computing. For a given Hamiltonian I calculated explicitly the eigenvalues . Worked out the details of how to add a constant energy gap using the stabilizer formalism [NC]. I have explicitly calculated

the eigenvalues for the encoded Hamiltonian for JFS codes that protect against 1 - local errors and then extended it for 2-local errors. For calculating the eigenvalues for the encoded case techniques used were of stabilizer formalism.

I have studied the error model used in [JFS] and [CFP02] . The evolution equation is of Lindblad [CFP02] form and stems from the coupling of each qubit in the adiabatic quantum computer to an harmonic oscillator bath. The master equation for the evolution is

$$\frac{d\rho}{dt} = -i[H_S, \rho] - \sum_{a,b} M_{ab}\varepsilon_{ab}(\rho) \tag{5}$$

where M_{ab} is a scalar,

$$\varepsilon_{ab}(\rho) = |a\rangle\langle a|\rho + \rho|a\rangle\langle a| - 2|b\rangle\langle a|\rho|a\rangle\langle b| \tag{6}$$

is an operator and a, b are the eigenstates of $H(S)$. Under the following model is I have numerically simulated the adiabatic passage through the point of smallest gap in the presence of a bath of local harmonic oscillators.

Contents

Chapter 1

Introduction and Preliminaries

1.1 Elements of Quantum Information

Information can be identified as the most general thing which must propagate from a cause to an effect. It therefore has a fundamentally important role in physics however, the mathematical treatment of information, especially information processing, is quite recent, dating from the mid-twentieth century. This has meant that the full significance of information as a basic concept in physics is only now being discovered. This is especially true in quantum mechanics. The theory of quantum information and computing puts this significance on a firm footing, and has lead to some profound and exciting new insights into the natural world. Among these are the use of quantum states to permit the secure transmission of classical information *quantum cryptography*, the use of quantum entanglement to permit reliable transmission of quantum states *teleportation*, the possibility of preserving quantum coherence in the presence of irreversible noise processes *quantum error correction*, and the use of controlled quantum evolution for efficient computation (quantum computation). The common theme of all these insights is the use of *quantum entanglement* as a computational resourIt turns out that information theory and quantum mechanics fit together very well. It turns out that information theory and quantum mechanics fit together very well. In order to explain their relationship, this review begins with an introduction to classical information theory and computer science, including *Shannon theorem*, *error correcting codes*, *Turing machines* and *computational complexity*. The principles of quantum mechanics are then outlined, and the EPR experiment described. The EPR-Bell correlations, and quantum entanglement in

general, form the essential new ingredient which distinguishes quantum from classical information theory, and, arguably, quantum from classical physics.

There are three very important features of quantum mechanics which provides us the way to exploit such powerful processors:

1. A quantum particle can exist simultaneously in many incompatible states.
2. We can operate on a quantum particle while it is in a superimposed state and affect all the states at once.
3. One quantum system can influence another far away quantum system instantaneously

This is the kind of parallelism inherent in quantum world and combined with the present day information processing gives birth to exciting developments: Quantum computation, quantum error correction, quantum entanglement and teleportation and quantum cryptography. Quantum computers are able to solve some problems intractable to conventional computation (problems like prime factorization and discrete logarithm). Quantum error correcting techniques enable us to do quantum computation and communication in present of noise. Quantum cryptosystems provide guaranteed secure communication using no-cloning theorem and uncertainty principle and quantum teleportation provides the way to do quantum communication in absence of a quantum channel using prior quantum entanglement and classical communication.

1.1.1 Model of quantum Computation

Basic requirements that should be present in any model of computation are :

1. Scheme for information representation
2. Set of legal operations
3. Methods of extracting result after the operation

In the quantum mechanical model of information processing the information is mathematically represented by a unit vector in a Hilbert Space , operations are the unitary operators in the space and result is the measurement of an observable described by a hermitian operator in the space.

Qubits and quantum registers

The first postulate of quantum mechanics sets up the arena in which quantum mechanics takes place. This area linear algebra,Hilbert space.

Postulate 1: Associated to any isolated physical system is a Hilbert space known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit (ray) in the systems's state space.

The simplest non-trivial Hilbert space is of dimension two and a state vector in the state space of dimension two is called a *qubit* (stands for a quantum bit). Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for that state space. Then an arbitrary state vector in the state space can be written

$|\psi\rangle = a|0\rangle + b|1\rangle$,

where a and b are complex numbers. The condition that $|\psi\rangle$ be a unit (ray), $\langle\psi|\psi\rangle = 1$, is therefore equivalent to $|a|^2 + |b|^2 = 1$.

Nature is not so simple and a qubit is not sufficient to deal with its complexity. We must be interested in composite system made of two (or more) distinct physical systems and we must also have a mathematical way of playing around with them. In analogy to the classical terminology, a composite quantum system i.e. a set of qubits is called a *quantum register*. The following postulate describes how the state space of a composite system (quantum register)is built up from the state spaces of the component systems (the qubits).

Postulate 2: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and a number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \bigotimes |\psi_2\rangle \bigotimes \ldots \bigotimes |\psi_n\rangle$, where $\bigotimes$ denotes tensor product.

Quantum gates

Time evolution of a quantum state is unitary; it is generated by a self-adjoint (Hermitian) operator, called the *Hamiltonian* of the system. In the *Schrodinger picture* of dynamics, the vector describing the system moves in time as governed by the *Schrodinger equantion*

$\frac{d}{dt}|\psi(t)\rangle = -i\mathbf{H}|\psi(\mathbf{t})\rangle$

where $\mathbf{H}$ is the Hamiltonian. We may express this equation, to first order in the infinitesimal quantity dt, as

$|\psi(t+dt)\rangle = (1 - i\mathbf{Hdt})|\psi(\mathbf{t})\rangle$.

Clearly, the operator $\mathbf{U(dt)} \equiv \mathbf{1 - iHdt}$ is unitary. Thus the time evolution over a finite interval is unitary given by

$|\psi(t)\rangle = \mathbf{U(t)}|\psi(\mathbf{0})\rangle$.

Postulate 3: The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$|\psi'\rangle = U|\psi\rangle$.

Now that a quantum system evolves according to a unitary operator which is always invertible, *quantum gates* must be reversible. Infact, quantum gates are nothing but these unitary operations. Following are some commonly used one qubit and two qubit gates in terms of their unitary operations represented by matrices in the computational basis.

Pauli's Gates (Operators) :

$\sigma_x \equiv$

$$\begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array}$$

$\sigma_y \equiv$

$$\begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \end{array}$$

$\sigma_z \equiv$

$$\begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{array}$$

Hadamard Gate :

$H \equiv$

$$\begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \end{array}$$

Controlled- NOT (CNOT) Gate: A two qubit gate

$$\begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

The Postulate 3 requires that the system being described be closed. That is, it is not interactive in any way with other systems. In reality, of course, all systems (except the Universe as a whole) interact at least somewhat with the other systems. Nevertheless, there are interesting systems which can be described by unitary evolution to some good approximation. Furthermore, at least in principle every open system can be described as part of a larger closed system (the Universe) which is undergoing unitary evolution.

Quantum measurement

An observable is a property of a physical system that in principle can be measured. In quantum mechanics, an observable is a hermitian operator. We also know that a hermitian operator in a Hilbert space $\mathbf{H}$ has a spectral decomposition- it's eigenstates form a complete orthonormal basis in $\mathbf{H}$. We can express a hermitian operetor $\mathbf{A}$ as

$\mathbf{A} = \sum_{\mathbf{n}} \mathbf{a_n P_n}$.

Here each a_n is an eigen value of $\mathbf{A}$, and $\mathbf{P_n}$ is the corresponding orthogonal projection onto the space of eigenvectors with eigenvalues a_n. (If a_n is non-degenerate, then $\mathbf{P_n} = |\mathbf{n}\rangle\langle\mathbf{n}|$; it is the projection onto the corresponding eigenvector.) The $\mathbf{P_n}$ satisfy

$\mathbf{P_n P_m} = \delta_{\mathbf{n},\mathbf{m}} \mathbf{P_n}$

$\mathbf{P_n^\dagger} = \mathbf{P_n}$.

Postulate 4: In quantum mechanics, the numerical outcome of a measurement of the observable $\mathbf{A}$ is an eigenvalue of $\mathbf{A}$; right after the measurement, the quantum state is

an eigenstate of $\mathbf{A}$ with the measured eigenvalue. If the quantum state just prior to the measurement is $|\psi\rangle$, then the outcome a_n is obtained with the *probability*

$\mathbf{Prob(a_n)} = \| \mathbf{P_n}|\psi\rangle \|^{\mathbf{2}} = \langle\psi|\mathbf{P_n}|\psi\rangle$;

If the outcome attained is a_n, then the (normalized) quantum state becomes $\frac{\mathbf{P_n}|\psi\rangle}{\sqrt{(\langle\psi|\mathbf{P_n}|\psi\rangle)}}$.

(Note that if the measurement is immediately repeated, then according to this rule the same outcome is attained again, with probability one.)

1.1.2 Quantum entanglement

Quantum mechanics builds systems out of subsystems in a remarkable, holistic way. The states of the subsystems do not determine the state of the system. Schrodinger, commenting on the EPR paper[**?**] in 1935, the year it appeared, coined the term *entanglement* for this aspects of quantum mechanics.

Consider a system consisting of two subsystems. Quantum mechanics associates to each subsystem a Hilbert space. Let $\mathbf{H_A}$ and $\mathbf{H_B}$ denote these two Hilbert spaces; let $|i_A\rangle$ (where i=1,2,...) represent a complete orthonormal basis for $\mathbf{H_A}$, and $|i_B\rangle$ (where i=1,2,...) represent a complete orthonormal basis for $\mathbf{H_B}$. Quantum mechanics asociates to the system-i.e. the two subsystem taken together-the Hilbert space $\mathbf{H_A} \bigotimes \mathbf{H_B}$, namely the Hilbert space spanned by the states $|i_A\rangle \bigotimes |i_B\rangle$. In the following we will drop the tensor product symbol $\bigotimes$ and write $|i_A\rangle \bigotimes |i_B\rangle$ as $|i_A\rangle|i_B\rangle$.

Any linear combinations of the basis states $|i_A\rangle|i_B\rangle$ is a state of the system, any state $|\psi\rangle_{AB}$ of the system can be written as

$|\psi\rangle_{AB} = \sum_{i,j} c_{i,j}|i_A\rangle|i_B\rangle$,

where the $c_{i,j}$ are complex coefficients, we take $|\psi\rangle_{AB}$ to be normalized, hence $\sum_{i,j} |c_{i,j}|^2 = 1$.

A special case of the above state is a *direct product* state in which $|\psi\rangle_{AB}$ factors into (a tensor product of) a normalized state $|\psi^{(A)}\rangle_A = \sum_i c_i^{(A)}|i\rangle_A$ in $\mathbf{H_A}$ and a normalized state $|\psi^{(B)}\rangle_B = \sum_j c_j^{(B)}|j\rangle_B$ in $\mathbf{H_B}$.

$|\psi\rangle_{AB} = |\psi^{(A)}\rangle_A|\psi^{(B)}\rangle_B = (\sum_i c_i^{(A)}|i\rangle_A)(\sum_j c_j^{(B)}|j\rangle_B)$

Not every state in $\mathbf{H_A} \bigotimes \mathbf{H_B}$ is a product state. Take, for example, the state $(|1\rangle_A|1\rangle_B + |2\rangle_A|2\rangle_B)/\sqrt{2}$; if we try to write it as a direct product of states of $\mathbf{H_A}$ and $\mathbf{H_B}$, we will find that we can *not*.

If $|\psi\rangle_{AB}$ is not a product state, we say that it is *entangled*.

Thus when two quantum subsystems are entangled, we may have a complete knowledge of the composite system as a whole but not of the individual subsystems. Technically speaking, the system as a whole may be in a *pure* state while individual subsystems still being in *mixed* states.

Entanglement is a key resource for quantum information processing and spatially separated entangled pairs of particles have been used for numerous purposes like teleportation [**?**], superdense coding and cryptography based on Bell's Theorem [**?**], to name a few. We shall see some novel and interesting characterization and applications of entanglement in this thesis.

1.1.3 The density operator

The *density operator* language provides a convenient means for describing quantum systems whose state is not completely known. More precisely, suppose a quantum system is in one of a number of states $|\psi_i\rangle$, where i is an index, with respective probabilities p_i. We shall call $\{p_i, |\psi_i\rangle\}$ an ensemble of pure states. The density operator for the system is defined by the equation

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{1.1}$$

Suppose, for example, that the evolution of a closed quantum system is described by the unitary operator U. Then the evolution of the density operator is described by the equation

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i| \longrightarrow^U \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger = U\rho U^\dagger \tag{1.2}$$

where $U^\dagger$ is the *Hermitian adjoint* of U. Measurements are also easily described in the density operator language. Suppose we perform a measurement described by measurement operators M_m. If the initial state was $|\psi_i\rangle$, then the probability of getting result

m is

$$\begin{aligned} p(m|i) &= \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle \\ &= tr\left(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|\right) \end{aligned} \tag{1.3}$$

By the law of total probability the probability of obtaining the result m is

$$\begin{aligned} p(m) &= \sum_i p(m|i)p_i \\ &= \sum_i p_i tr\left(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|\right) \\ &= tr\left(M_m^\dagger M_m\rho\right). \end{aligned} \tag{1.4}$$

Density operator of the system after obtaining the measurement result m is

$$\rho_m = \frac{M_m\rho M_m^\dagger}{tr\left(M_m^\dagger M_m\rho\right)} \tag{1.5}$$

1.1.4 Shannon entropy

One of the most important concept of classical information theory is *Shannon entropy*. For a given *random variable* X the Shannon entropy of X quantifies how much information we gain, on average, when we learn the value of X. An alternative view is that the entropy of X measures the amount of *uncertainty* about X before we learn its value. These two views are complementary; we can view entropy either as a measure of our uncertainty *before* we learn the value of X,or as a measure of how much information we have gained *after* we learn the value of X.

The information content of a random variable should not depend on the labels attached to the diffrent values that may be taken by the random variable. For example, we expect that the random variable taking the values $'heads'$ and $'tails'$ with respective probabilities 1/4 and 3/4 contains the same amount of information as a random variable that take the values 0 and 1 with respective probabilities 1/4 and 3/4. For this reason, the entropy of a random variable is defined to be a function of the probabilities of the diffrent possible values the random variable takes, and is not influenced by the labels used for those values. We often write the entropy as a function of a probability distribution, $p_1, \ldots, p_n$. The Shannon entropy associated with this probability distribution is

defined by

$$H(X) \equiv H(p_1, \ldots, p_n) \equiv -\sum_x p_x \log p_x \tag{1.6}$$

1.1.5 Von Nuemann entropy

The Shannon entropy measure the uncertainty associated with a classical probability distribution. Quantum states are described in a similar fashion, with density operators replacing probability distributions. In this section we generalize the definition of the Shannon entropy to quantum states.

Von Neumann defined the it entropy of a quantum state ρ by the formula

$$S(\rho) = -tr(\rho \log \rho_2) \tag{1.7}$$

If λ_x are the eigenvalues of ρ then von Neumann's definition can be re-expressed

$$S(\rho) = -\sum_x \lambda_x \log \lambda_x, \tag{1.8}$$

where we define $0 \log 0 \equiv 0$.

Suppose ρ and σ are the density operator of two quantum states. Then *relative entropy* of ρ to σ is defined by

$$S(\rho||\sigma) \quad equiv \quad tr(\rho \log \rho) - tr(\rho \log \sigma). \tag{1.9}$$

Basic properties of von Nuemann entropy:

1. *Klein's inequality:*The quantum relative entropy is non-negative,

$$S(\rho||\sigma) \geq 0, \tag{1.10}$$

   with equality if and only if $\rho = \sigma$.

2. The entropy is non-negative. The entropy is 0 if and only if the state is pure.

3. In the d-dimensional Hilbert space the entropy is at most $\log d$.

4. Suppose a composite system AB is pure state. Then $S(A) = S(B)$.

5. Suppose p_i are probabilities, and the states ρ_i on orthogonal subspaces. Then

$$S\left(\sum_i p_i \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i). \tag{1.11}$$

6. *Joint entropy theorem:* Suppose p_i are probabilities, $|i\rangle$ are orthogonal states for s system A, and ρ_i is any set of density operators for another system, B. Then

$$S\left(\sum_i p_i |i\rangle\langle i| \otimes \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i). \tag{1.12}$$

1.2 Adiabatic Computation

Since the paradigm of adiabatic quantum computation (AQC) was established by Farhi [EJSM], there have been two successive "waves". The first wave was initiated by the inventor, the second wave by the paper of Aharonov et al. [DA] who showed that the adiabatic and the circuit model for quantum computation are, in fact, equivalent in power.

1.2.1 Adiabatic quantum computation, old style

According to the Adiabatic Theorem (explained later), a ground-state of a Hamiltonian $H(0)$ is prepared and then the Hamiltonian $H(s)$ is slowly and continuously varied through the interval $0 \leq s \leq 1$,

$$H(t) = (1 - s)H_i + sH_f. \tag{1.13}$$

The initial Hamiltonian H_i is chosen such that its ground state is easy to prepare and the Hamiltonian H_f is chosen such that its ground state contains the answer to a computational problem. The idea is that if the Hamiltonian is varied slowly enough then the instantaneous ground state follows adiabatically. That is, the system remains in its ground state throughout the evolution and, in particular, is found in the ground state at $s = 1$.

The question is: How slow is slow enough? The conditions for the adiabatic theorem require that $\dot{s} \approx \Delta(s^{-2})$ where Δ is the ground state energy gap at s. Thus, the run-time of the adiabatic algorithm depends critically on the minimum ground state energy gap, and it is important to know how $min_s(\Delta(s))$ scales with the problem size (= number of qubits required).

To pin down this scaling is possible only in very special cases as it basically amounts to diagonalizing a very large Hamiltonian (matrix). The scaling is known e.g. for an adiabatic version of Grover search where it yields a quadratic speedup, comparable to Grover's original algorithm.

Now, what about fault-tolerance in this scenario? It has often been stated that adiabatic quantum computation is inherently robust against noise because the ground state energy gap Δ is protecting it; See eg. Childs and Preskill [CFP02]. In more detail, the argument is that, first, the adiabatic algorithm is robust against phase errors in the instantaneous eigenbasis of $H(s)$ because the system is in an energy eigenstate state. Second, the the adiabatic algorithm is protected against excitations into higher energy states of the instantaneous eigenbasis by the ground state energy gap.

Third, the adiabatic algorithm is robust against perturbations of the Hamiltonian $H(s)$ as long as these are sufficiently slowly varying with s and are small at $s = 0$ and $s = 1$.

The problem is above item No. 2, protection by the ground state energy gap. For all so far investigated cases, there is one point s_0 in the adiabatic procedure where $\Delta(s_0)$ becomes very small. Because of the adiabaticity condition $\dot{s} \approx \Delta(s_{-2})$ this is the point where the algorithm spends most of its time. This situation is disadvantages from the viewpoint of fault-tolerance, because at s_0 where the gap is small excitations to higher-energy states are not suppressed by a favorable Bolzmann factor. Rather, $e^{-\Delta(s_0)/kBT} \approx 1$ for $T > \Delta(s_0)$. So, excitations into higher energy eigenstates are not energetic ally suppressed and all time on earth is available for them to happen. This is like preserving a snowball in the center of the sun from the sun's creation to the present.

1.2.2 Adiabatic quantum computation, new style

This line started with Kempe et al.'s work showing that the adiabatic and the circuit model are computationally equivalent. Building on that framework, Shor et al. [JFS] showed that a constant energy gap against local and near-local errors can be obtained.

Now, a constant-size gap is no guarantee for error-correction. A prominent example is the surface code. It protects reliably against error in the case of active error-correction where the complete error syndrome is measured once every constant-time interval [D01]. To the contrary, in a passive error-correction scenario where the code space is the ground state manifold of a suitably chosen Hamiltonian, protected by a constant-size gap, error-correction breaks down [AL07].

1.3 Quantum Cellular Automata

Implementation of quantum systems for computing and information processing is one of the most difficult hurdle in the field of Quantum Computing and Information. Symmetric designs of quantum systems reduce implementation complexity to great extent. Recently great progress have been made in realization of optical lattices or arrays of micro-lenses which for the time being have been important candidates for for implementation of qubits. All these objects possess a translation symmetry in arrangements of qubits and their mutual interaction. *Quantum Cellular Automata* (QCA) represents a suitable framework for studying the computational power of these physical systems as they respect these symmetries (translation invariant).

So it becomes very important to know that computational strength of QCA and it has been shown that 1-dimensional QCA cab efficiently simulate a quantum *Turing Machine* [JW95]. Further more it has been shown that there exist a universal QCA that can simulate any other automaton with linear slowdown [WVM96]. Question that still remains open is that of fault tolerance. A quantum computation model should be fault tolerant to have practical importance as all quantum systems are under the influence of decoherence and neighborhood coupling. We will here propose a design QCA which will be able to detect and correct errors.

1.4 Thesis Contribution and Organization

Chapter 2

Adiabatic Theorem and Adiabatic Quantum Computing

2.1 Adiabatic Theorem

Every quantum system evolves according to the continuous time dependent Schroedinger equation

$$\frac{d|\phi(t)\rangle}{dt} = iH(t)|\phi(t)\rangle \tag{2.1}$$

with a continuous time-dependent Hamiltonian $H(t)$, and the eigen states of (2.1) are called the *energy states* of the Hamiltonian, with the respective eigen values as *energies*. The adiabatic theorem [Messiah76] tells us how a quantum system evolves when the time dependent Hamiltonian $H(t)$ is slowing varying with time. Before we can state the adiabatic theorem we need to define some terms that will be required for stating the theorem.

Let us consider a smooth family of Hamiltonian $\bar{H(s)}$ where $0 \leq s \leq 1$, and take

$$H(t) = \bar{H}(t/T) \tag{2.2}$$

so T controls the rate at which $H(t)$ varies. The eigen states and eigen values of $\bar{H(s}$ are given by

$$\bar{H}(s)|l;s\rangle = E_l(s)|l;s\rangle \tag{2.3}$$

with

$$E_0(s) \leq E_1(s) \leq \cdots \leq E_{N_1}(s) \tag{2.4}$$

where N is the dimension of the Hilbert space. Then according to the adiabatic theorem if $|\phi(0)\rangle = |l = 0; s = 0\rangle$ i. e, if we start with the ground state of the initial Hamiltonian $\bar{H}(0)$ and if the energy gap between the two lowest levels, $E_1(s) - E_0(s)$, is nonzero for all $0 \leq s \leq 1$, then

$$\lim_{T\to\infty} |\langle l = 0; s = 1|\phi(T)| = 1. \tag{2.5}$$

This implies that the existence of a nonzero gap will make sure that $|\phi(t)\rangle$ of (2.1) remains close to the instantaneous ground state of $H(t)$ (2.2) if for all $0 \leq t \leq T$ if T is large enough.

Though the above result look very impressive but it wont help much in developing quantum algorithm as there is no bound on the size of T. We will here give a popular version or folk theorem that is normally stated while developing adiabatic quantum algorithm. For the exact statement refer to the appendix at the end of this chapter or [AO06].

THEOREM 2.1.1 [Adiabatic theorem, folk version]
Let $\bar{H}(s)$ be a time-dependent Hamiltonian and

$$g_{min} = \min_{0\leq s\leq 1} (E_1(s) - E_0(s)) > 0, \tag{2.6}$$

$$\epsilon = \max_{0\leq s\leq 1} |\langle l = 1; s|\frac{d\bar{H}(s)}{ds}|l = 0; s\rangle| \tag{2.7}$$

then by taking $T \gg \frac{\epsilon}{g_{min}^2}$ we can make $|\langle l = 0; s = 1|\phi(T)\rangle| \approx 1$.

Normally the adiabatic algorithm that will be discussed here are the ones where the ϵ is of the order of eigen values of H hence not too large, so the size of T will depend on the order of g_{min}.

2.2 Adiabatic Quantum Computing

Since adiabatic theorem has been stated now we are in a position to discuss quantum algorithms using the principle of adiabatic evolution. Any adiabatic quantum algorithm for a given problem consists of the following steps:

1. An easily constructed initial state ψ which is the ground state of an Hamiltonian H_i.

2. A time-dependent Hamiltonian $H(s)$ (2.2), which can be constructed from an problem instance. We also have to take care that the $H(s)$ satisfies (2.6), $H(0) = H_i$ and the ground state of the final Hamiltonian H(1) encodes the solution of the problem.

3. Apply the Hamiltonian to ψ for time T for long enough (as given in the Theorem 2.1.1) so that the final state is very close to the ground state of $H(1)$.

4. Measurement of the state gives the result.

The main problem with adiabatic algorithm is to construct a continuous family of Hamiltonian whose initial ground state encodes the problem instance and final ground states encodes solution to the problem. To make the algorithm feasible for implementation and computationally interesting the size of T should be of the order of $poly(n)$, where n is the size of the input. One of the most important questions is that can adiabatic quantum computation solve a computationally difficult problem in polynomial time. There are enough evidence to say that it wont be able to solve an NP-complete problem in polynomial time [], but it will be very interesting to investigate for problems in the class $NP - P$ which are not NP-complete. Now we will present adiabatic algorithms [EJSM] for solving $3 - SAT$-problem and Grover search problem.

2.3 Equivalence of AQC to Standard Model

Aharonov et al. in there paper "Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation " [DA] showed that Adiabatic Quantum Computation is polynomially equivalent to the *Circuit Model* of quantum computation.

THEOREM 2.3.1 [DA] the model of adiabatic computation is polynomially equivalent to the standard model of quantum computation.

Theorem 2.3.1 uses 3-local Hamiltonian that act on particles that may be arbitrarily far apart. For a practical point of view, it is very difficult to create controlled interaction between two particle that are far apart from each other. In addition, 3-local Hamiltonian

are very difficult to realize. On the other hand 2-local Hamiltonians with nearest neighbor interaction have been implemented efficiently in the labs. In the paper [DA] also proved that theorem for 2-local Hamiltonians with nearest neighbor interaction.

THEOREM 2.3.2 [DA] Any quantum computation can be efficiently simulated by adiabatic computation with 2-local nearest neighbor Hamiltonians operating on 6-state particles set on a two dimensional grid.

2.4 Adiabatic Grover Search

In this section we will consider the Grover problem [Grover97]. We have a single clause h_G, which depends on all n bits with a unique but unknown satisfying assignment $w = (w_1, w_2, \ldots, w_n)$. Classical we cannot do it better than $O(2^n)$ but Grover [Grover97] showed that it can be done in $O(2^{\frac{n}{2}})$ using quantum computing model (circuit model) and it has also been shown to be tight. Here we will present a adiabatic search algorithm whose order is same as that of classical bound.

Corresponding problem to the h_G we have the problem Hamiltonian

$$H_P|z_1 z_2 \ldots z_n\rangle = \begin{cases} |z_1 z_2 \ldots z_n\rangle & \text{if } |z_1 z_2 \ldots z_n\rangle \neq |w_1 w_2 \ldots w_n \\ 1 & \text{if } |z_1 z_2 \ldots z_n\rangle = |w_1 w_2 \ldots w_n \end{cases} \tag{2.8}$$

$$= 1 - |z = w\rangle\langle z = w| \tag{2.9}$$

We can write $\bar{H}(s)$ explicitly as

$$\bar{H}(s) = \bar{H}(s) = (1-s)\sum_{j=1}^{n} \frac{1}{2}(1-\sigma_x)(j) + s(1 - |z = w\rangle\langle z = w|). \tag{2.10}$$

Consider the transformation given by

$$|z_1\rangle|z_2\rangle \ldots |z_n\rangle \longrightarrow |z_1'\rangle|z_2'\rangle \ldots |z_n'\rangle \quad \begin{cases} z_j' = \bar{z_j} & \text{, if } w_j = 1 \\ z_j' = z_j & \text{, if } w_j = 0. \end{cases} \tag{2.11}$$

Under this transformation $\bar{H}(s)$ becomes

$$\bar{H}(s) = \bar{H}(s) = (1-s)\sum_{j=1}^{n} \frac{1}{2}(1-\sigma_x)(j) + s(1 - |z = w\rangle\langle z = w|). \tag{2.12}$$

As the two Hamiltonians are unitarily equivalent they have the same spectra and accordingly the same g_{min}. Hence we will study the second one.

The ground state of $\bar{H}(0)$ is $|x=0\rangle$, which is symmetric under the interchange of any two bits. Also the Hamiltonian (2.12) is symmetric under the interchange of any two bits. Instead of working in the 2^n-dimensional space we can work in the $(n+1)$-dimensional subspace of symmetrized states.

Define $\overrightarrow{S} = (S_x, S_y, S_z)$ by

$$S_a = \frac{1}{2}\sum_{j=1} n\sigma_a^{(j)} \tag{2.13}$$

for $a = x, y, z$. The symetrical states have $\overrightarrow{S}_2$ equal to $\frac{n}{2}(\frac{n}{2}+1)$, where $\overrightarrow{S}_2 = S_x^2+S_y^2+S_z^2$. The states can be characterize as the states of S_x or S_z

$$S_x|m_x = m\rangle = m|m_x = m\rangle \qquad m = -\frac{n}{2}, -\frac{n}{2}+1, \ldots, m = -\frac{n}{2} \tag{2.14}$$

$$S_z|m_z = m\rangle = m|m_z = m\rangle \qquad m = -\frac{n}{2}, -\frac{n}{2}+1, \ldots, m = -\frac{n}{2} \tag{2.15}$$

where the total spin is suppressed as it remains constant. In terms of the z basis states

$$|m_z = \frac{n}{2} - k\rangle = \binom{n}{k} \sum_{z_1+z_2+\cdots+z_n=k} |z_1\rangle|z_2\rangle \ldots |z_n\rangle \tag{2.16}$$

for $k = 0, 1, 2, \ldots, n$. In particular

$$|m_z = \frac{n}{2}\rangle = |z = 0\rangle. \tag{2.17}$$

One can rewritten as $\tilde{H}(s)$ in (2.10) as

$$\tilde{H}(s) = (1-s)[\frac{n}{2} - S_x] + s[1 - |m_z = \frac{n}{2}\rangle\langle m_z = \frac{n}{2}]. \tag{2.18}$$

Now the problem has been reduced to finding s of an $(n+1)$-dimensional matrix $\tilde{H}(s)$ for which the gap between the two smallest eigen values is minimum.

Let the eigen vector corresponding to the eigen value E of the Hamiltonian $\tilde{H}(s)$ be ψ. Then we have

$$\tilde{H}(s) = E\psi, \tag{2.19}$$

taking dot product on both side of (2.19) with $|m_x = \frac{n}{2} - r\rangle$ we get

$$[s + (1-s)r]\big\langle m_x = \frac{n}{2} - r\big|\psi\big\rangle - s\big\langle m_x = \frac{n}{2} - r\big|m_z = \frac{n}{2}\big\rangle = E\big\langle m_x = \frac{n}{2} - r\big|\psi\big\rangle. \tag{2.20}$$

If E is replaced by the variable λ where $E = s + (1-s)\lambda$, multiplying by $\langle m_z = \frac{n}{2}|m_x = \frac{n}{2} - r$ and sum over r to get

$$\frac{(1-s)}{s} = \sum_{r=0}^{n} \frac{1}{r-\lambda} P_r, \quad \text{where} \quad P_r = |\langle m_z = \frac{n}{2}|m_x = \frac{n}{2} - r\rangle|^2. \tag{2.21}$$

Using (2.16) with $k = 0$ and also the identical formula with z replaced with x we have

$$P_r = \frac{1}{2^n}\binom{n}{r}. \tag{2.22}$$

The left-hand side of (2.20) ranges over all positive values as s varies from 0 to 1. Take $s = s^*$ such that

$$\frac{(1-s^*)}{s^*} = \sum_{r=1}^{n} \frac{P_r}{r}. \tag{2.23}$$

Eigenvalue equation (**??**) at $s = s^*$ becomes

$$\frac{P_0}{\lambda} = \sum_{r=1}^{n} P_r \frac{\lambda}{r(r-\lambda)}. \tag{2.24}$$

From (2.22) we know that $P_0 = 2^{-n}$. Define u by $\lambda = 2^{-n/2}u$. Then (2.24) becomes

$$\frac{1}{u} = \sum_{r=1}^{n} P_r \frac{u}{r(r - 2^{-n/2}u)} \approx \sum_{r=1}^{n} P_r \frac{u}{r^2} \tag{2.25}$$

hence

$$\lambda \approx \pm(\sum_{r=1}^{n} \frac{P_r}{r^2})^{-\frac{1}{2}} 2^{\frac{-n}{2}} \tag{2.26}$$

, which implies

$$g_{min} = 2(1-s^*)(\sum_{r=1}^{n} \frac{P_r}{r^2})^{-1/2} 2^{-n/2}. \tag{2.27}$$

We know that

$$\sum_{r=1}^{n} \frac{P_r}{r^2} = \frac{4}{n^2} + O(\frac{1}{n^3}). \tag{2.28}$$

Using (2.28) and (2.27) we get

$$g_{min} \approx 2.2^{-\frac{n}{2}}. \tag{2.29}$$

Since the running time is $O(\frac{1}{g_{min}^2})$ hence running time for the adiabatic algorithm is $O(2^n)$.

2.5 3-SAT Problem

An instance of 3-SAT satisfiability problem is a boolean formula

$$C_1 \wedge C_2 \wedge \cdots \wedge C_m \tag{2.30}$$

where $C_r = x_i \vee x_j \vee x_k$ and x_i, x_j, x_k are literals of the boolean formula. The Hamiltonian for the 3-SAT problem takes the form

$$H(t) = H_{C_1}(t) + H_{C_2}(t) + \cdots + H_{C_n}(t) \tag{2.31}$$

where each H_{C_i} depends only on the clause C_i and acts on the bits corresponding to the literals of C_i. The initial state is the ground state of $H(0)$ and for each i, the ground state of $H_{C_i}(T)$ encodes the satisfying assignments of the clause C_i hence ground state of $H(T)$ encodes the satisfying assignment for the boolean formula if there is one.

An n bit instance of 3-SAT boolean formula (2.30) is specified by a collection of clauses and each clauses contain 3 of the n bits. The three bits associated with the clause C are marked as i_C, j_C, k_C and for each clause there is an *energy function* [EJSM]

$$h_C(z_{i_C}, z_{j_C}, z_{k_C}) = \begin{cases} 0 & \text{if } (z_{i_C}, z_{j_C}, z_{k_C}) \text{ satisfies the clause } C; \\ 1 & \text{if } (z_{i_C}, z_{j_C}, z_{k_C}) \text{ does not satisfy the clause } C; \end{cases} \tag{2.32}$$

where z_i denotes the bits that can take values 0 or 1 and i runs from 1 to n. Then the total energy function h is defined as

$$h = \sum_C h_C. \tag{2.33}$$

Total energy function $h \geq 0$ and $h(z_1, z_2, \ldots, z_n) = 0$ if and only if $(z_1, z_2, \ldots, z_n)$ satisfies the 3-SAT formula. Thus finding the minimum energy level of h will tell us if the 3-SAT formula is satisfiable or not.

Having given the brief idea we are now in a position to give the details of the adiabatic algorithm to [EJSM] solve 3-SAT problem.

Problem Hamiltonian

When we make a transition from classical to quantum computation we have already seen that we replace the classical bit z_i by a spin-$\frac{1}{2}$ qubit labeled by $|z_i\rangle$ where $z_i = 0, 1$. the

states $|z_i\rangle$ are eigen states of the z component of the the i^{th} spin,

$$\frac{1}{2}(1-\sigma_z^{(i)})|z_i\rangle = z_i|z_i\rangle. \tag{2.34}$$

The Hilbert space for the quantum computation is a complex vector space spanned by $N = 2^n$ basis vectors $|z_1\rangle|z_2\rangle\ldots|z_n\rangle$. Each clause C of the 3-SAT boolean formula is associated with the operator $H_{P,C}$.

$$H_{P,C}(|z_1\rangle|z_2\rangle\ldots|z_n\rangle) = h_C(z_{i_C}, z_{j_C}, z_{k_C})|z_1\rangle|z_2\rangle\ldots|z_n\rangle \tag{2.35}$$

where h_C is the *energy function* defined previously. The Hamiltonian associated with the problem is

$$H_P = \sum_C H_{P,C}. \tag{2.36}$$

H_P by construction is a *positive-semidefinite* matrix i.e, $\langle\phi|H_P|\phi\rangle \geq 0 \;\forall\; |\phi\rangle$ and $H_P|\phi\rangle = 0$ if and only if ϕ is the superposition of states $|z_1\rangle|z_2\rangle\ldots|z_n\rangle$ where $z_1, z_2, \ldots, z_n$ satisfy all the clauses hence the problem instance. So solving the 3-SAT is equivalent is equal to finding the ground state of the Hamiltonian H_P.

Initial Hamiltonian

Now we will construct Hamiltonian H_B which will be easy to construct and whose ground state is simple to find. Let $H_B^{(i)}$ be the Hamiltonian acting on the i-th bit

$$H_B^{(i)} = \frac{1}{2}(1-\sigma_x^{(i)}) \tag{2.37}$$

so

$$H_B^{(i)}|x_i = x\rangle = x|x_i = x\rangle \tag{2.38}$$

where

$$|x_i = 0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{and} \quad |x_i = 1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.39}$$

For each clause associated with the bits i_C, j_C, and k_C we have

$$H_{B,C} = H_B^{(i_C)} + H_B^{(j_C)} + H_B^{(k_C)} \tag{2.40}$$

and

$$H_B = \sum_C H_{B,C}. \tag{2.41}$$

The ground state of H_B is $|x_1 = 0\rangle|x_2 = 0\rangle\ldots|x_n = 0\rangle$. The important feature of the ground state is that it is a equal superposition of all 2^n basis vectors $|z_1\rangle|z_2\rangle\ldots|z_n\rangle$ which is easy to construct.

Adiabatic Evolution

We will now go from the known ground state of H_B to the unknown ground state of H_P. Consider

$$H(t) = (1 - t/T)H_B + (t/T)H_P, \tag{2.42}$$

so prepare the system so that it begins at $t = 0$ in the ground state of $H_(0) = H_B$. And the Adiabatic theorem will ensure that if g_{min} is non zero and T is large enough then the final ground state $\phi(T)$ will be very close to the ground state of H_P, which is the solution of the 3-SAT problem.

2.6 Illustration of instances of 3-SAT problem.

We will here work out the details of the 3-SAT problem for the particular case

$$P(x_1, x_2, x_3) = (x_1 + x_2 + x_3)(\bar{x_1} + \bar{x_2} + x_3). \tag{2.43}$$

Lets take

$$\begin{aligned} C_1 &= (x_1 + x_2 + x_3) \quad \text{and} \\ C_2 &= (\bar{x_1} + \bar{x_2} + x_3). \end{aligned}$$

Then

$$H_{P,C_1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{2.44}$$

and

$$H_{P,C_2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2.45}$$

So the problem Hamiltonian $H_P = H_{P,C_1} + H_{P,C_2}$

$$H_P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2.46}$$

And the initial Hamiltonian

$$H_B = (1 - \sigma_x^1) + (1 - \sigma_x^2) + (1 - \sigma_x^3)$$

$$H_B = \begin{pmatrix} 1.5 & -0.5 & -0.5 & 0 & -0.5 & 0 & 0 & 0 \\ -0.5 & 1.5 & 0 & -0.5 & 0 & -0.5 & 0 & 0 \\ -0.5 & 0 & 1.5 & -0.5 & 0 & 0 & -0.5 & 0 \\ 0 & -0.5 & -0.5 & 1.5 & 0 & 0 & 0 & -0.5 \\ -0.5 & 0 & 0 & 0 & 1.5 & -0.5 & -0.5 & 0 \\ 0 & -0.5 & 0 & 0 & -0.5 & 1.5 & 0 & -0.5 \\ 0 & 0 & -0.5 & 0 & -0.5 & 0 & 1.5 & -0.5 \\ 0 & 0 & 0 & -0.5 & 0 & -0.5 & -0.5 & 1.5 \end{pmatrix} \tag{2.47}$$

The plot of the eigenvalues shows that 6 eigenvalues converge 0 at $t = 1$, which should be the case as the number of solutions of the instance of 3-SAT is 6 in this case.

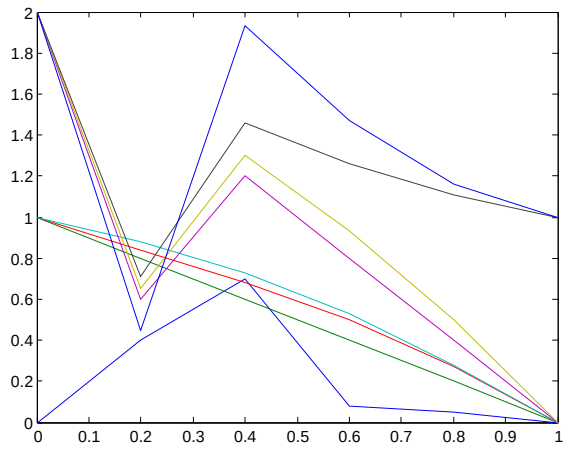

Figure 2.6.1: Plot of Eigenvalues of $H(T)$ vs Time.

Appendix A.

THEOREM 2.6.1 [AO06]
Let $H(s)$, $0 \leq 1$ be a time dependent Hamiltonian, let $E(s)$ be one of its eigenstates, and let $e(s)$ be the corresponding eigenvalue. Assume that for any $s \in [0,1]$, there is no eigenvalues of $H(s)$ lying between $[e(s) - \lambda, e(s) + \lambda]$. Consider the adiabatic evolution given H and ϕ applied for time T. Then, the following condition is enough to guarantee that the final state is at distance at most δ from $\phi(1)$:

$$T \geq \frac{10^5}{\delta^2}.max\left(\frac{||H'||^3}{\lambda^4}, \frac{||H'||.||H''||}{\lambda^3}\right).$$

Chapter 3

Quantum Error Correcting codes

This chapter develops a general framework for studying quantum error-correction, including quantum error-corrections and conditions which must be satisfied if quantum error correction is possible.

Quantum states are encoded by a unitary operation into a *quantum error-correcting code* which is a subspace C of a larger Hilbert space. The projector onto the code space is denoted by P. After the encoding is done the system is subjected to noise which is followed by a sequence of measurements which are called *syndrome measurements*. This is done to know the kind of errors that have occurred and it is called the *error syndrome*. Once the error sequence is obtained a recovery operation is done to return the quantum system to the original state. Different error syndrome takes the state to different subspace of the Hilbert and the subspace so that the syndrome measurements wont be able to distinguish between the different errors. Furthermoe, the different subspaces must be undeformed versions of the original code space, in the sense that the errors mapping to the different subspaces must take the codewords to orthogonal states, in order to be able to recover from errors.

The *quantum error-correction conditions* are a set of conditions which must be satisfied by a error-correcting code to protect against particular type of errors $\mathcal{E}$. These conditions has been used to construct different types of error correcting codes, and also to investigate general properties of error correcting codes.

THEOREM 3.0.2 (**Quantum error-correction conditions** [NC]) Let C be a quantum code, and let P be the projector onto C. Suppose $\mathcal{E}$ is a quantum operation with operational elements E_i. A necessary and sufficient version condition for the existence

of an error-correction operation $\mathcal{R}$ correcting $\mathcal{E}$ on C is that

$$PE_i^\dagger E_j P = \alpha_{ij} P, \tag{3.1}$$

for some Hermitian matrix α of complex numbers.

3.1 Discretization of errors

The previous Theorem 3.0.2 gives the required conditions for protection against specific noises (errors). In general, one does not know exactly what noise is acting on a quantum system. It would be useful if a specific code C and error-correction operation $\mathcal{R}$ could be used to protect against an entire class of noises. The next theorem will give a more detail account on the conditions that needs to be satisfied to make this possible.

THEOREM 3.1.1 [NC] Suppose C is a quantum code and $\mathcal{R}$ is the error-correction operation of the Theorem 3.0.2. to recover from a noise process $\mathcal{E}$ with operational elements E_i. Suppose $\mathcal{F}$ is a quantum operation with operational elements F_j which are linear combinations of E_i i. e, $F_j = \sum_i m_i E_i$ where m_i are complex numbers. Then the error-correction operation $\mathcal{R}$ also corrects for effects of the noise process $\mathcal{F}$ on the code C.

3.2 Quantum error-correction without measurement

Normally quantum error-correction is a two stage process: error detection step which is done by using quantum measurement and recovery step after the detection which is effected by conditioned unitary operations. It is also possible to perform quantum error-correction using only unitary operations and ancilla systems prepared in the standard states. This is important experimentally because it is easier to perform unitary operation than measurements.

Suppose that syndrome measurement on the principal system which is being error-corrected by the measurement operators M_i, and the corresponding conditional unitary operation is U_i. Introduce an ancilla system with basis states $|i\rangle$ corresponding to the possible error syndromes. The ancilla starts in a standard pure state $|0\rangle$ before error

correction. An unitary operator U is defined on the principal system plus ancilla by

$$U|\phi\rangle|0\rangle = \sum_i (U_i M_i |\phi\rangle)|i\rangle. \tag{3.2}$$

This can be extended to a unitary operator acting on the whole space since

$$\begin{aligned} \langle\phi|\langle 0|U^\dagger U|\psi\rangle|0\rangle &= \sum_{ij} \langle\phi|M_i^\dagger M_j|\psi\rangle\delta_{ij} && (3.3)\\ &= \sum_i \langle\phi|M_i^\dagger M_i|\psi\rangle && (3.4)\\ &= \langle\phi|\psi\rangle. && (3.5) \end{aligned}$$

This shows that U preserves inner products, and can be extended to a unitary operator on the entire state space. The effect of U is to effect the transformation $\mathcal{R}(\sigma) = \sum_\rangle \mathcal{U}_\rangle \mathcal{M}_\rangle \sigma \mathcal{M}_\rangle^\dagger \mathcal{U}_\rangle^\dagger$ on the space being error corrected, exactly the same quantum operation as described in the main text for the performance of quantum error-correction. Note that in order for this error-correction procedure to work it is necessary to use new ancilla each time error-correction is performed.

3.3 Stabilizer code

Stabilizer codes [NC] are important class of quantum error correcting codes whose construction is analogous to *classical linear codes*. Before we introduce stabilizer codes let us explain the idea of *stabilizer formalism*. Group theory is an important technique used in the development stabilizer formalism. The group of principal interest is the *Pauli Group* G_n on n qubits. G_1 is defined as follows

$$G_1 \equiv \pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ. \tag{3.6}$$

The group of matrices G_1 forms a group under the operation of matrix multiplication. Therefore G_n is defined as a recursively

$$G_n = G_{n-1} \otimes G_1. \tag{3.7}$$

Now we are in a position to define stabilizer. Suppose S be a Abelian subgroup of G_n and we define V_S as the those set of n-qubit states which are fixed by every element

of S, and S is said to be the stabilizer of the space V_S. And in other word V_S is said to be the stabilizer code for the subgroup S.

Property of the Stabilizer formalism.

1. Every linear combination of the elements of V_S is also in V_S. V_S is a vector space.
2. Suppose S is a subgroup of G_n with generators $g_1, \ldots, g_n$ then S is abelian iff g_i and g_j commute for each pair of i, j.
3. Let $S = \left\langle g_1, \ldots, g_{n-k} \right\rangle$ be generated by $n-k$ independent and commuting elements from G_n, and such that $-I \notin S$. Then v_S is a 2^k-dimensional vector space.

Unitary Gates and the Stabilizer formalism

Suppose we apply a unitary operation U to a vector space V_S stabilized by the group $S \subset G_n$. Let ϕ be any element of V_S. Then for any element of g of S,

$$U|\phi\rangle = Ug|\phi\rangle = UgU^\dagger U|\phi\rangle \tag{3.8}$$

thus the state $U|\phi\rangle$ is stabilized by $UgU^\dagger$, so we can deduce that the vector space $USU^\dagger \equiv UgU^\dagger | g \in S$. If the generators S were $g_1, \ldots, g_k$ then the generators of the $USU^\dagger$ are $Ug_1U^\dagger, \ldots, Ug_kU^\dagger$. *Clifford Group* C_n on n-qubits is defined as

$$C_n = U | UgU^\dagger \in G_n \text{ where } g \in G_n. \tag{3.9}$$

Clifford group also plays an important part in fault tolerance of quantum systems.

The Gottesman-Knill Theorem

The results to describe unitary gates and measurements using stabilizer code can the summarized in the Gottesman-Knill theorem:

THEOREM 3.3.1 **(Gottesman-Knill Theorem)** [NC] Suppose a quantum computation is performed which involves only the following elements: state preparations in the computational basis, Hadamard gates, phase gates, controlled-NOT gates, Pauli gates, and measurements of observables in the Pauli group (which includes measurements in the computational basis as a special case), together with the possibility of classical control conditioned on the outcome of such measurements. Such a computation may be efficiently simulated on a classical computer.

Chapter 4

Error Correcting code for AQC and Error Model Analysis

In this chapter we will discuss the work done on error-correcting codes for Adiabatic Quantum Computation (AQC) [JFS] and will use the results to show how we can add energy gap to a given Hamiltonian. We will also explicitly calculate the new eigenvalues of the encoded Hamiltonian in Section 4.1. We will also present a brief description of the *Ising Hamiltonian* and its diagonalisation using *Jordan-Wigner transformations* in Section . Error Model, it analytic analysis for the encoded case and numerical analysis of the error model for the unencoded case using *Ising Hamiltonian* has been done in Section 4.3. Before we start with the error model analysis we give a brief introduction to Stabilizer code for AQC.

4.1 Stabilizer Code for AQC

Adiabatic quantum computing has an inherently fault-tolerant because of the energy gap provides to some extent resistance to noise caused by stray coupling to the environment. A system goes to an excited state from the ground state if k_bT is less than the energy gap where T is the temperature of the system. Most of the known adiabatic quantum algorithm has the energy gap scaling as an inverse polynomial of the problem size. This energy gap would provide protection if the temperature shrinks in the same way but that may be hard to achieve experimentally.

To make sure that an adiabatic evolution has at least a constant energy gap against

1-local noises, Jordan et al. [JFS] had come up with an encoding scheme to tackle this problem using stabilizer codes that protects against 1-local noises. By 1-local noises means Pauli operators acting on individual qubits. To do this they have used a quantum error correcting code such that any one local noise will send the code word out of the codespace. The main goal here is to add energy penalty for the states lying outside the codespace. So the error correcting code is not actually an error correcting code but an error *detecting* code.

The 4-qubit code stabilizer code that protects against 1-local noises is

$$\begin{aligned} |0_L\rangle &= \frac{1}{2}(|0000\rangle + i|0011\rangle + i|1100\rangle + |1111\rangle), \\ |1_L\rangle &= \frac{1}{2}(|0101\rangle + i|0110\rangle + i|1001\rangle + |1010\rangle). \end{aligned} \tag{4.1}$$

$$\tag{4.2}$$

This satisfies the error detection requirements

$$\langle 0_L|\sigma|0_L\rangle = \langle 1_L|\sigma|1_L\rangle = \langle 0_L|\sigma|1_L\rangle = 0 \tag{4.3}$$

where σ is any of the three pauli operators acting on one qubit. The 4-qubit code will be used to encode each qubit of the original Hamiltonian.

The logical Pauli operators X, Y, Z acting on the code space are,

$$\begin{aligned} X_L &= Y \otimes I \otimes Y \otimes I, \\ Y_L &= -I \otimes X \otimes X \otimes I, \\ Z_L &= Z \otimes Z \otimes I \otimes I. \end{aligned} \tag{4.4}$$

That is,

$$\begin{aligned} X_L|0_L\rangle = |1_L\rangle, \qquad & X_L|1_L\rangle = |0_L\rangle \\ Y_L|0_L\rangle = i|1_L\rangle, \qquad & Y_L|1_L\rangle = -i|0_L\rangle \\ Z_L|0_L\rangle = |0_L\rangle, \qquad & X_L|1_L\rangle = -|1_L\rangle. \end{aligned} \tag{4.5}$$

The generators of the stabilizer group or the code given in (4.1) are

$$\begin{aligned} g_1 &= X \otimes X \otimes X \otimes X \\ g_1 &= Z \otimes Z \otimes Z \otimes Z \\ g_1 &= X \otimes Y \otimes Z \otimes I \end{aligned} \tag{4.6}$$

We already know that 2-local Hamiltonian is universal for quantum computation [DA]. So starting with a 2-local Hamiltonian acting on N qubits we get a new fault tolerant 4-local Hamiltonian acting on $4N$ qubits. Since any 2-local Hamiltonian H is sum of tensor product of pairs of Pauli matrices acting on different qubits. We use following transformations

$$X \to X_L, \quad Y \to Y_L, Z \to Z_L \tag{4.7}$$

on the old 2-local Hamiltonian H to obtain the new 4-local Hamiltonian H_{SL} acting on $4N$ qubits. The total Hamiltonian H_S is given by

$$H_S = H_{SL} + H_{SP} \tag{4.8}$$

where H_{SP} is the sum of energy penalty term acting on each qubit. The energy penalty for each qubit is at least E_P for going out of the codespace.

Adding on eterm of the form

$$H_P = -E_P(g_1 + g_2 + g_3) \tag{4.9}$$

to the encoded qubit will ensure an energy penalty of at least E_P for states out of the codespace.

If the ground space of H is spanne by $|\psi^{(1)}rangle \ldots |\psi^{(1)}\rangle$ then the ground state of H_{SL} is spanned by the states $|\psi_L^{(1)}rangle \ldots |\psi_L^{(1)}\rangle$. Since H_{SL} and H_{SP} commute thus they share a set of simultaneous eigenstates.

THEOREM 4.1.1 Given an Hamiltonian H with eigenvalues λ_j then the eigenvalues of H_S are of the form

$$\lambda_j - E_P * \sum_{i=1}^{N} (\pm 1 \pm 1 \pm 1) \tag{4.10}$$

where E_P is the energy penalty for going out of the codespace and N is number of qubits.

PROOF. Let the initial Hamiltonian be H acting on N qubnits, then the fault tolerant Hamiltonian H_S is given by

$$H_S = H_{SL} + H_{SP} \tag{4.11}$$

where H_{SL} is obtained by replacement of the Pauli matrices of the original Hamiltonian by

$$\begin{aligned} X &\to X_L, \\ Y &\to Y_L, \\ Z &\to Z_L \end{aligned} \tag{4.12}$$

and

$$\begin{aligned} H_{SP} &= \sum_{i=1}^{N} H_P^{(i)} \\ &= \sum_{i=1}^{N} -E_P(S_{1,i} + S_{2,i} + S_{3,i}). \end{aligned} \tag{4.13}$$

In (4.13) $g_{k,l}$ denotes the stabilizer generator acting on the qubit l.

The basis of the encoded space is $\{|\bar{i}\rangle = |\lambda_z, s_1, s_2, s_3\}$ where

$$\begin{aligned} &Z_L|\bar{i}\rangle = \lambda_z|\bar{i}\rangle, \\ &S_k = s_k|\bar{i}\rangle, \quad \text{for} \quad k = 1, 2, 3. \\ &s_i, \lambda_z \in \{1, -1\} \end{aligned} \tag{4.14}$$

Here Z_L is the logical Z of the encoded logical qubits. Thus, in particular,

$$|0_L\rangle = |+1, +1, +1, +1\rangle, \text{ and} \tag{4.15}$$

$$|1_L\rangle = |-1, +1, +1, +1\rangle \tag{4.16}$$

are the logical $|0\rangle$ and $|1\rangle$ respectively.

Using the stabilizer as introduced in Section 3.3 the encoded basis state for $4N$-qubits is given by

$$|\bar{i_1} \ldots |\bar{i_N}\rangle = |\bar{i_1}\rangle \otimes \cdots \otimes |\bar{i_N}\rangle. \tag{4.17}$$

Lets take the special case when $|\bar{i_k}\rangle$, $|\bar{j_l}\rangle \in \{|\bar{0}\rangle, |\bar{1}\rangle\}$, then

$$\begin{aligned}
\langle \bar{j_1} \dots \bar{j_N}|H_S|\bar{i_1} \dots \bar{i_N}\rangle = \quad & \langle \bar{j_1} \dots \bar{j_N}|H_{SL}|\bar{i_1} \dots \bar{i_N}\rangle \\
& -\langle \bar{j_1} \dots \bar{j_N}|H_{SP}|\bar{i_1} \dots \bar{i_N}\rangle \\
= \quad & \langle \bar{j_1} \dots \bar{j_N}|H_{SL}|\bar{i_1} \dots \bar{i_N}\rangle \\
& -\langle \bar{j_1} \dots \bar{j_N}|\Big(\sum_{k=1}^{N} S_{i_k}\Big)|\bar{i_1} \dots \bar{i_N}\rangle \\
= \quad & e_{ij}(H) - 3N * E_P \langle \bar{j_1} \dots \bar{j_N}|\bar{i_1} \dots \bar{i_N}\rangle \\
= \quad & e_{ij}(H) - 3N * E_P * \delta_{ij} \qquad (4.18)
\end{aligned}$$

where $i = i_1 \dots i_N$, $j = j_1 \dots j_N$, $S_k = S_{1,k} + S_{2,k} + S_{3,k}$.

Now for the general case, let the new basis be defined under the stabilizer formalism as $|\bar{i}\rangle \in \{|\lambda_z, \bar{S_i}\rangle : \bar{S_i} = (S_{1,i}, S_{2,i}, S_{3,i})\}$ where $S_{i,j} = \pm 1$ and $S_k = S_{1,i} + S_{2,i} + S_{3,i}$. Using the above notation we have,

$$\begin{aligned}
\langle \bar{j_1} \dots \bar{j_N}|H_S|\bar{i_1} \dots \bar{i_N}\rangle = \quad & \langle \bar{j_1} \dots \bar{j_N}|H_{SL}|\bar{i_1} \dots \bar{i_N}\rangle \\
& -\langle \bar{j_1} \dots \bar{j_N}|H_{SP}|\bar{i_1} \dots \bar{i_N}\rangle \\
= \quad & \langle \bar{j_1} \dots \bar{j_N}|H_{SL}|\bar{i_1} \dots \bar{i_N}\rangle \\
& -\langle \bar{j_1} \dots \bar{j_N}|(\sum_{k=1}^{N} S_{i_k})|\bar{i_1} \dots \bar{i_N}\rangle \\
= \quad & e_{ij}(H) - \Big(\sum_{k=1}^{N} S_{i_k}\Big)\langle \bar{j_1} \dots \bar{j_N}|\bar{i_1} \dots \bar{i_N}\rangle \\
= \quad & e_{ij}(H) - \Big(\sum_{k=1}^{N} S_{i_k}\Big) * E_P * \delta_{ij}. \qquad (4.19)
\end{aligned}$$

Hence the Hamiltonian H_S in the new basis transforms into

$$H_S = H \otimes I_{2^{3N}} - I_{2^N} \otimes E_{2^{3N}}, \qquad (4.20)$$

where H, I_{2^N} act on the first qubit and $I_{2^{3N}}$, $E_{2^{3N}}$ act on the last three bits of each encoded qubit of the new basis. $E_{2^{3N}}$ is a diagonal matrix with $E_{2^{3N}}(SS) = \sum_{i=1}^{N} S_{i_k}$ where $S = S_{i_1} \dots S_{i_N}$. Hence the diagonal entries of $E_{2^{3N}}$ are of the form $\sum i = 1^N(\pm 1 \pm 1 \pm 1)$.

Let U diagonalizes H then take $\bar{U} = U \otimes I_{2^{3N}}$. So,

$$\begin{aligned}\bar{U}^\dagger H_S \bar{U} &= \bar{U}^\dagger H \otimes I_{2^{3N}} \bar{U} - \bar{U}^\dagger I_{2^{3N}} \otimes E_{2^{3N}} \bar{U} \\ &= U^\dagger H U \otimes I_{2^{3N}} - U^\dagger I_{2^{3N}} U \otimes E_{2^{3N}} \\ &= U^\dagger H U \otimes I_{2^{3N}} - I_{2^{3N}} \otimes E_{2^{3N}} \end{aligned} \tag{4.21}$$

Therefore $\bar{U}$ diagonalizes H_S. Hence the eigen values of H_S are of the form

$$\lambda_j - E_P * \sum_{i=1}^{N} (\pm 1 \pm 1 \pm 1), \quad \text{where } \lambda \text{ is an eigenvalue of } H. \tag{4.22}$$

□

We have presented 4-qubit stabilizer code [JFS] which adds constant energy gap against 1-local noise. Now we present a 5-qubit stabilizer code [JFS] that protect against 2-local errors and also adds a constant energy gap to the Hamiltonian. The 5-qubit code stabilizer code that protects against 2-local noise is

$$\begin{aligned}|0_L\rangle = \quad & \frac{1}{4}[|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \\ & + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ & - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ & - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle] \end{aligned} \tag{4.23}$$

$$\begin{aligned}|1_L\rangle = \quad & \frac{1}{4}[|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle \\ & + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\ & - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle \\ & - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle]. \end{aligned} \tag{4.24}$$

$$\tag{4.25}$$

The encoded Pauli operators are for the code are

$$\begin{aligned} X_L &= -X \otimes I \otimes Y \otimes Y \otimes I, \\ Y_L &= -Z \otimes Z \otimes I \otimes Y \otimes I, \\ Z_L &= -Y \otimes Z \otimes Y \otimes I \otimes . \end{aligned} \tag{4.26}$$

The generators of the stabilizer group for code are

$$\begin{aligned} g_1 &= X \otimes Z \otimes Z \otimes X \otimes I, \\ g_2 &= I \otimes X \otimes Z \otimes Z \otimes X, \\ g_3 &= X \otimes I \otimes X \otimes Z \otimes Z, \\ g_4 &= Z \otimes X \otimes I \otimes X \otimes Z. \end{aligned} \tag{4.27}$$

4.2 Ising Hamiltonian

Transverse Ising model is given by the equation

$$H(t) = -t \sum_{i=1}^{n} \sigma_x^i - (1-t) \sum_{i=1}^{n} \sigma_z^i \sigma_z^{i+1} \tag{4.28}$$

where σ_t, $t = x, y, z$ are the Pauli matrices and, $\sigma_z^{n+1} = \sigma_z^1$. Transverse Ising model can be considered as a adiabatic quantum algorithm, even though the problem that it solves is the problem of finding numbers with all the bits same. It will be shown later in the section that the energy gap between two lowest eigenvalues is non-zero so it is a case of adiabatic evolution.

4.2.1 Diagonalisation of Ising Hamiltonian

For diagonalisation of the of Ising Hamiltonian we use *Jordan-Wigner transformation* [SS] to replace σ_x^i and σ_z^i by *Fermi oprators* $(1 - 2c_i^\dagger c_i)$ and $-\Pi_{j<i}(1 - 2c_i^\dagger c_i)(c_i + c_i^\dagger)$, where

$$\begin{aligned} c_i &= \left(\Pi_{j<i}\sigma_z^j\right)\left(\sigma_x^i + i\sigma_y^i\right)/2 \quad \text{and} \\ c_i^\dagger &= \left(\Pi_{j<i}\sigma_z^j\right)\left(\sigma_x^i - i\sigma_y^i\right)/2. \end{aligned} \tag{4.29}$$

Substituting the values in (4.28) we get the Ising Hamiltonian in the quadratic in the Fermi operators:

$$H(t) = -(1-t) \sum_i \left(c_i^\dagger c_{i+1} + c_{i+1}^\dagger c_i + c_i^\dagger c_{i+1}^\dagger + c_i c_{i+1} - 2\frac{t}{1-t} c_i^\dagger c_i - \frac{t}{1-t} \right) \tag{4.30}$$

Using the the momentum eigenstates

$$c_k = \frac{1}{\sqrt{M}} \sum_j c_j e^{-ik_j}, \tag{4.31}$$

where M is the number of sites, to get

$$H(t) = (1-t)\sum_k \Big(2[\frac{t}{1-t} - cos(ka)]c_k^\dagger c_k - isin(ka)[c_{-k}^\dagger c_k^\dagger + c_{-k}c_k] - \frac{t}{1-t}\Big). \quad (4.32)$$

Next using *Bogoliubov transformation* [SS] we map to a new set of fermionic operators (γ_k). These new operators are defined by a unitary transformation on the pair $c_k, c_k^\dagger$:

$$\gamma_k = u_k c_k - iv_k c_k^\dagger, \quad (4.33)$$

where $u_k = cos(\theta k/2)$ and $u_k = sin(\theta k/2)$ and

$$tan\theta_k = \frac{sin(ka)}{cos(ka) - \frac{t}{1-t}}. \quad (4.34)$$

The final form of the diagonalized Hamiltonian is

$$\epsilon_k = 2(1-t)\Big(1 + \frac{t^2}{(1-t)^2} - 2\frac{t}{1-t}cosk\Big)^{1/2}. \quad (4.35)$$

4.2.2 Numerical Stimulation of Ising model

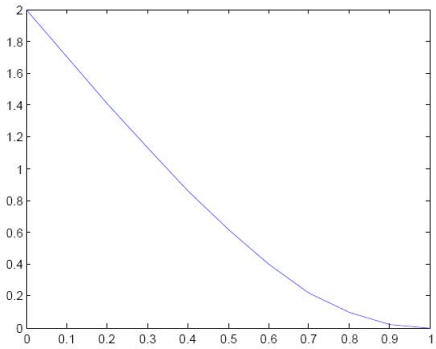

Figure 4.2.1: Plot of Energy gap between two lowest eigenvalues for $N = 2$.

4.3 Error Model and Analysis

We describe here a model of decoherence from [JFS, CFP02] and show that how 4-qubit stabilizer code [JFS] protects against 1-local errors. The evolution equation is of *Lindbald*

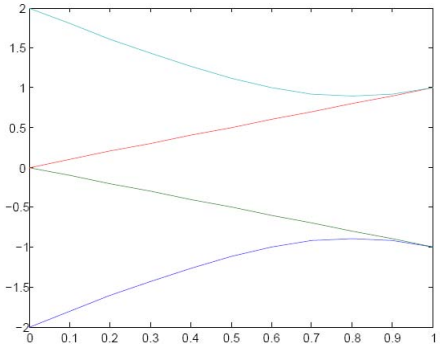

Figure 4.2.2: Plot of Eigenvalues of Ising Hamiltonian for $N = 3$.

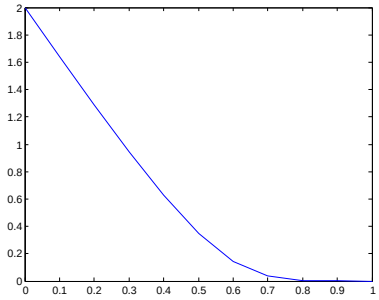

Figure 4.2.3: Plot of Energy gap between two lowest eigenvalues for $N = 3$.

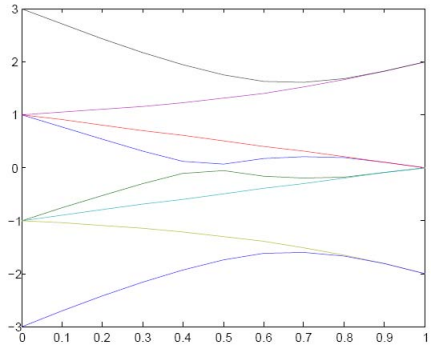

Figure 4.2.4: Plot of Eigenvalues of Ising Hamiltonian for $N = 3$.

form and stems from coupling of each qubit in the adiabatic quantum computer to an *Harmonic* oscillator. Let ρ be the density natrix of the N-qubit quantum state and H_S be the Hamiltonian acting on the system, then

$$\frac{d\rho}{dt} = -i[H_S, \rho] - \sum_{a,b} M_{ab} E_{ab}(\rho) \tag{4.36}$$

where

$$\begin{aligned} M_{ab} &= \sum_i \Big[N_{ba} |g_{ba}|^2 \langle a|\sigma_-^{(i)}|b\rangle\langle b|\sigma_+^{(i)}|a\rangle \\ &\quad + (N_{ab}+1)|g_{ab}|^2 \langle b|\sigma_-^{(i)}|a\rangle\langle a|\sigma_+^{(i)}|b\rangle \Big] \end{aligned}$$

is a scalar,

$$E_{ab}(\rho) = |a\rangle\langle a|\rho + \rho|a\rangle\langle a| - 2|b\rangle\langle a|\rho|a\rangle\langle b| \tag{4.37}$$

is an operator, $|a\rangle$ is the instantaneous eigenstate of H_S with energy ω_a,

$$N_{ba} = \frac{1}{\exp\left[\beta(\omega_b - \omega_a)\right] - 1} \tag{4.38}$$

is the Bose-Einstein distribution at temperature $1/\beta$, and

$$g_{ba} = \begin{cases} \lambda g(\omega_b - \omega_a), & \omega_b > \omega_a, \\ 0, & \omega_b \leq \omega_a. \end{cases} \tag{4.39}$$

4.3.1 Analysis for the Encoded case

Suppose that we encode the original N-qubit Hamiltonian as a $4N$-qubit Hamiltonian as described above. As stated in equation **??**, the total spin Hamiltonian H_S on $4N$ spins consists of the encoded version H_{SL} of the original Hamiltonian H_S plus the penalty terms H_{SP}.

Most adiabatic quantum computations use an initial Hamiltonian with an eigenvalue gap of order unity, independent of problem size. In such cases, a nearly pure initial state can be achieved at constant temperature. Therefore, we'll make the approximation that the spins start in the pure ground state of the initial Hamiltonian, which we'll denote $|0\rangle$. Then we can use equation 4.36 to examine ρ/t at $t = 0$. Since the initial state is $\rho = |0\rangle \langle 0|$, $E_{ab}(\rho)$ is zero unless $|a\rangle = |0\rangle$. The master equation at $t = 0$ is therefore

$$\left.\frac{d\rho}{dt}\right|_{t=0} = -i[H_S, \rho] - \sum_b M_{0b} E_{0b}(\rho). \tag{4.40}$$

H_{SP} is given by a sum of terms of the form **??**, and it commutes with H_{SL}. Thus, H_S and H_{SP} share a complete set of simultaneous eigenstates. The eigenstates of H_S can thus be separated into those which are in the codespace C (i. e, the ground space of H_{SP}) and those which are in the orthogonal space $C^\perp$. The ground state $|0\rangle$ is in the codespace. M_{0b} will be zero unless $|b\rangle \in C^\perp$, because $\sigma_\pm = (X \pm iY)/2$, and any Pauli operator applied to a single bit takes us from C to $C^\perp$. Equation 4.40 therefore becomes

$$\left.\frac{d\rho}{dt}\right|_{t=0} = -i[H_S, \rho] + \sum_{b \in C^\perp} M_{0b} E_{0b}(\rho) \tag{4.41}$$

Since $|0\rangle$ is the ground state, $\omega_b \geq \omega_0$, thus equation 4.53 shows that the terms in M_{0b} proportional to $|g_{0b}|^2$ will vanish, leaving only

$$M_{0b} = \sum_i N_{b0} |g_{b0}|^2 \langle 0|\sigma_-^{(i)}|b\rangle \langle b|\sigma_+^{(i)}|0\rangle. \tag{4.42}$$

Now let's examine N_{b0}.

$$\omega_b - \omega_0 = \langle b|(H_{SL} + H_{SP})|b\rangle - \langle 0|(H_{SL} + H_{SP})|0\rangle. \tag{4.43}$$

$|0\rangle$ is in the ground space of H_{SL}, thus

$$\langle b|H_{SL}|b\rangle - \langle 0|H_{SL}|0\rangle \geq 0, \tag{4.44}$$

and so

$$\omega_b - \omega_0 \geq \langle b|H_{SP}|b\rangle - \langle 0|H_{SP}|0\rangle. \tag{4.45}$$

Since $|b\rangle \in C^\perp$ and $|0\rangle \in C$,

$$\langle b|H_{SP}|b\rangle - \langle 0|H_{SP}|0\rangle = E_p, \tag{4.46}$$

thus $\omega_b - \omega_0 \geq E_p$.

A sufficiently large βE_p will make N_{ba} small enough that the term $\sum_{b\in C^\perp} M_{0b}E(\rho)$ can be neglected from the master equation, leaving

$$\left.\frac{d\rho}{dt}\right|_{t=0} \approx -i[H_S, \rho] \tag{4.47}$$

which is just Schrödinger's equation with a Hamiltonian equal to H_S and no decoherence.

4.3.2 Numerical Error Analysis for Unencoded Case

In this section we will numerically simulate the passage of Ising Hamiltonian for the case $N = 2$ in presence of harmonic oscillator bath.

We here again state the master equation for evolution, where ρ is the density matrix of the quantum system

$$\frac{d\rho}{dt} = -i[H_S, \rho] - \sum_{a,b} M_{ab}E_{ab}(\rho) \tag{4.48}$$

where

$$\begin{aligned} M_{ab} &= \sum_i \Big[N_{ba}|g_{ba}|^2 \langle a|\sigma_-^{(i)}|b\rangle\langle b|\sigma_+^{(i)}|a\rangle & (4.49)\\ &\quad + (N_{ab}+1)|g_{ab}|^2 \langle b|\sigma_-^{(i)}|a\rangle\langle a|\sigma_+^{(i)}|b\rangle \Big] & (4.50) \end{aligned}$$

is a scalar,

$$E_{ab}(\rho) = |a\rangle\langle a|\rho + \rho|a\rangle\langle a| - 2|b\rangle\langle a|\rho|a\rangle\langle b| \tag{4.51}$$

is an operator, $|a\rangle$ is the instantaneous eigenstate of H_S with energy ω_a,

$$N_{ba} = \frac{1}{\exp\left[\beta(\omega_b - \omega_a)\right] - 1} \tag{4.52}$$

is the Bose-Einstein distribution at temperature $1/\beta$, and

$$g_{ba} = \begin{cases} \lambda g(\omega_b - \omega_a), & \omega_b > \omega_a, \\ 0, & \omega_b \leq \omega_a. \end{cases} \tag{4.53}$$

H_S for our case is the Ising Hamiltonian for 2-qubits

$$H_I(t) = -(1-t)(X_1 + X_2) - tZ_1Z_2. \tag{4.54}$$

We take $\lambda = .0001$ and $\beta = 1$ for our numerical simulation. We will do the simulation for the initial state i. e, $t = 0$ and for point of smallest gap i. e, $t = 0.6$.

Evolution equation at $t = 0.6$

Eigenvalues of $H_I(0.6)$ are $-1, -0.6, 0.6, 1$ and the respective eigen vectors are

$$\begin{aligned}
|v_1\rangle = &\quad -0.6325|00\rangle - 0.3162|01\rangle - 0.3162|10\rangle - 0.6325|11\rangle \\
|v_2\rangle = &\quad -0.7071|00\rangle - 0.7071|11\rangle \\
|v_3\rangle = &\quad -0.7071|01\rangle - 0.7071|10\rangle \\
|v_4\rangle = &\quad 0.3162|00\rangle - 0.6325|01\rangle - 0.6325|10\rangle + 0.3162|11\rangle
\end{aligned} \tag{4.55}$$

Using (4.49) we get

$$\begin{aligned}
M_{v_1v_2} = &\quad 2.032 \times 10^{-7} \\
M_{v_1v_3} = &\quad 1.4354 \times 10^{-7} \\
M_{v_1v_4} = &\quad 1.0847 \times 10^{-7} \\
M_{v_2v_1} = &\quad -2.032 \times 10^{-7} \\
M_{v_2v_3} = &\quad 1.8932 \times 10^{-7} \\
M_{v_2v_4} = &\quad 1.7839 \times 10^{-7} \\
M_{v_3v_3} = &\quad -1.4354 \times 10^{-7} \\
M_{v_3v_2} = &\quad -1.8932 \times 10^{-7} \\
M_{v_3v_4} = &\quad 2.0537 \times 10^{-7} \\
M_{v_4v_1} = &\quad -1.0847 \times 10^{-7} \\
M_{v_4v_2} = &\quad -1.7839 \times 10^{-7} \\
M_{v_4v_3} = &\quad 2.0537 \times 10^{-7}
\end{aligned} \tag{4.56}$$

This set of equation shows that as λ is decreased in value we get closer and closer to the Schrödinger equation.

Chapter 5

Fault-Tolerant Quantum Cellular Automaton.

We are trying to implement fault tolerant quantum cellular automaton on the 2-dimensional surface codes [Kitaev03]. The qubits on the lattice edges will be the physical bits and the logical bits will be encoded in some way inside the surface code. The translation invariant operation will be on the physical layer to get the desired gates in the logical qubits. The operation that we are considering will be translation invariant in space only and not time.

5.1 Surface Code

We will first review some basic definitions of surface codes. In case of surface codes [Kitaev03] the physical qubits stay on the edges of the 2-dimensional lattice. To cause logical error on the encoded qubits (encoding of the logical qubits will be described later) the physical error should stretch a constant portion of the lattice. The topological structure will provides us with some sort fault-tolerance that will also be explained later.

The stabilizer elements of the code are associated with the faces f and the vertices or sites v of the lattice,

$$S_X(v) = \bigotimes_{e|\, v\in\{\partial e\}} X_e, \qquad S_Z(f) = \bigotimes_{e\in\{\partial f\}} Z_e. \tag{5.1}$$

Here, ∂ is the boundary operator of the cell complex. The number of logical qubits that can be stored in a surface codes depends on the boundary conditions, if the surface is a torus i. e, it has got a periodic boundary conditions ('toric code') then it can store two qubits, on the other hand if the surface has got 'rough edges' [KB], then they can store one logical qubits. For our case at least for now we do not enforce any boundary conditions, we will assume that the lattice lies in $\mathbb{R}^2$.

Now we will define two types of defects on the surface code each encoding two different types of qubits called electric and magnetic qubits. A electric and magnetic qubits are formed from the a pair of electric and magnetic holes. A magnetic hole is a plaquette f where the stabilizer $S_Z(f) = S_Z(f) = \bigotimes_{e\in\{\partial f\}} Z_e = Z(\partial f)$ associated with it is not enforced on the code space, while the electric hole is a site s where the associated stabilizer $S_X(s) = \bigotimes_{e|\, s\in\{\partial e\}} X_e = X(\partial \overline{s})$ is not enforced on the code space. Here $\overline{s}$ denotes the dual transformation on the dual lattice obtained by taking the sites as the faces of the original lattice. For a pair of magnetic holes f, f' the encoded σ_x operator is $\overline{X}^m = X(\overline{c_1})$, with $\partial\overline{c_1} = \{\overline{f}, \overline{f'}\}$, and the encoded phase flip operator is $\overline{Z}^m = Z(c_1)$, with $c_1 \cong \partial f$ or $c_1 = \partial f'$ and

$$Z(\partial f + \partial f') \in S. \tag{5.2}$$

Similarly for pair of electric holes s, s' we have $\overline{X}^e = X(\overline{c_1}')$, with $\overline{c_1}' \cong \partial\overline{s}$, $\overline{Z}^e = Z(c_1)$, with $\partial c_1 = \{s, s'\}$, and

$$X(\partial\overline{s} + \partial\overline{s'}) \in S. \tag{5.3}$$

Now with the encoding of the logical qubits fixed we can check if we can have the universal set of gates for quantum computation.

5.2 Universal set of gates

From the previous section we have already seen that have got encoded $\overline{X}, \overline{Z}$ for both magnetic and electric qubits. The operation *'Move'* defined in Appendix 5.4, will be used to move magnetic hole on the surface code. If one of the magnetic holes of a magnetic qubit is moved around a electric hole of an electric qubit, then we get a CNOT gate with the magnetic qubit as the control and electric qubit as the target [Kitaev03]. The problem with this gate is that these gates are abelian.

Figure 5.2.1 shows alternative circuit for the CNOT gates, where the control and target are both electric qubits and ancilla(3) is magnetic and ancilla(1) is electric. So

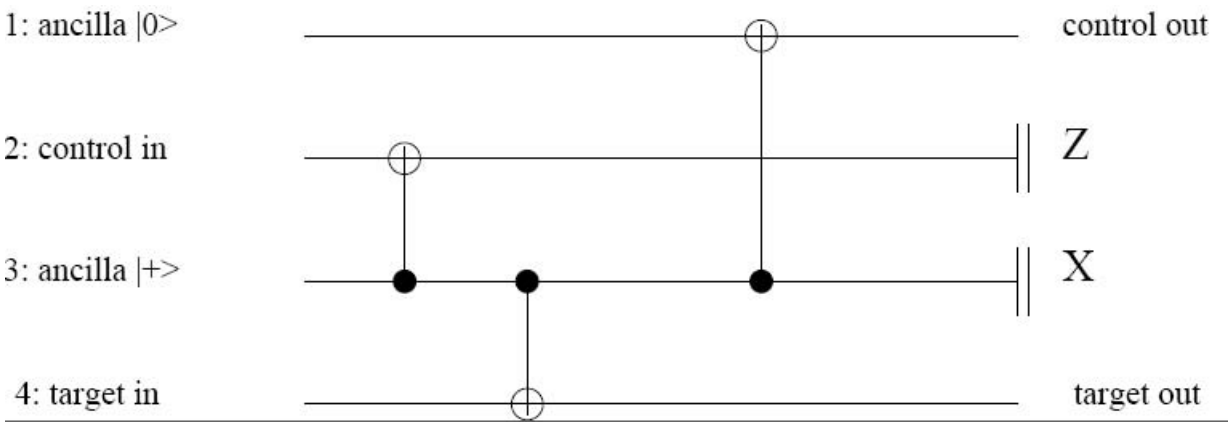

Figure 5.2.1: Equivalent circuit of CNOT as given in [RJK] page6.

now we can do CNOT with qubit of the same kind, and we obtain a non-abelian set of unitary gates.

The universal set of gates can be completed by adding $\exp(i\frac{\pi}{8}Z)$, $\exp(i\frac{\pi}{4}Z)$, $\exp(i\frac{\pi}{8}X)$. Fault tolerant realization of these gates require ancilla sates $|Y\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$ and $|A\rangle = (|0\rangle + e^{i\frac{\pi}{4}}|1\rangle)/\sqrt{2}$. These states are first created in a errornious fashion then distilled using variant of magic state distillation details of which are given in [KB05, RJK] and Appendix 5.5. The distilled ancillas will be used in implementation of the gates $\exp(i\frac{\pi}{8}Z)$, $\exp(i\frac{\pi}{4}Z)$, $\exp(i\frac{\pi}{8}X)$ [KB05].

5.3 Translation Invariant Gates and Measurements

After completing the universal set of gates for quantum computation the next problem is the arrangements of qubits on the surface code, implementation of the gates in a translation invariant manner and measurement of the error syndrome. The arrangements of the qubits on the surface and implementation of the gates in a translation invariant way are related problem. On the other hand syndrome measurement can be done irrespective of the way the above things are implemented.

5.3.1 Syndrome Measurements and correction

Measuring the plaquette operators: For measuring the plaquette operator we have a set of ancillas, there is one ancilla corresponding to each plaquette of the surface code.

Each ancilla a corresponding to the plaquette p are prepared in the state $|+\rangle$, then we do the following operation

$$\bigotimes_{i\in\partial p} \Lambda(Z)_{a,i}. \tag{5.4}$$

After that we do X measurement on the ancilla. If we get $+1$ then it is not an error syndrome if -1 then it is an error syndrome.

Measuring the site operators: For measuring the site operator we have a set of ancillas, there is one ancilla corresponding to each site of the surface code. Each ancilla b corresponding to the site s are prepared in the state $|+\rangle$, then we do the following operation

$$\bigotimes_{j\in\partial \overline{p}} \Lambda(X)_{b,j}. \tag{5.5}$$

After that we do X measurement on the ancilla. If we get $+1$ then it is not an error syndrome if -1 then it is an error syndrome.So we can see that syndrome measurements can be done in translation invariant way.

Error syndromes are processed classically using *minimum weight chain matching algorithm* [JED] for error correction.

5.3.2 Model 1: Simulation of one-dimensional cellular automaton on surface code

In this model we will try to simulate a one dimensional quantum cellular automaton on the surface code with specific properties. By specific properties we mean that number of plaquette in one column depends on the number of qubits in the input and the axis perpendicular to it will be fixed for time. In this construction the toric codes will have magic states $|H\rangle = \frac{(|0\rangle+e^{i\pi/4}|1\rangle)}{\sqrt[2]{2}}$ and $|S\rangle = \frac{(|0\rangle)+i|1\rangle}{\sqrt[2]{2}}$ placed periodically. The dual lattice of the code surface is shown in the Figure 5.3.2 where the logical qubit is encoded by pair of blue plaquettes, ancilla $|H\rangle$ is encoded by a pair of green plaquettes and $|S\rangle$ is encoded by pair of grey plaquette in the Figure 5.3.2.) are used for the implementation of the gates $\exp(i\frac{\pi}{8}Z)$, $\exp(i\frac{\pi}{4}Z)$ and $\exp(i\frac{\pi}{8}X)$. Together with X, Z and CNOT this completes the universal set of gates for quantum computation. These operation will be called *basic operations*. The period of A in the vertical axis and B in the horizontal axis

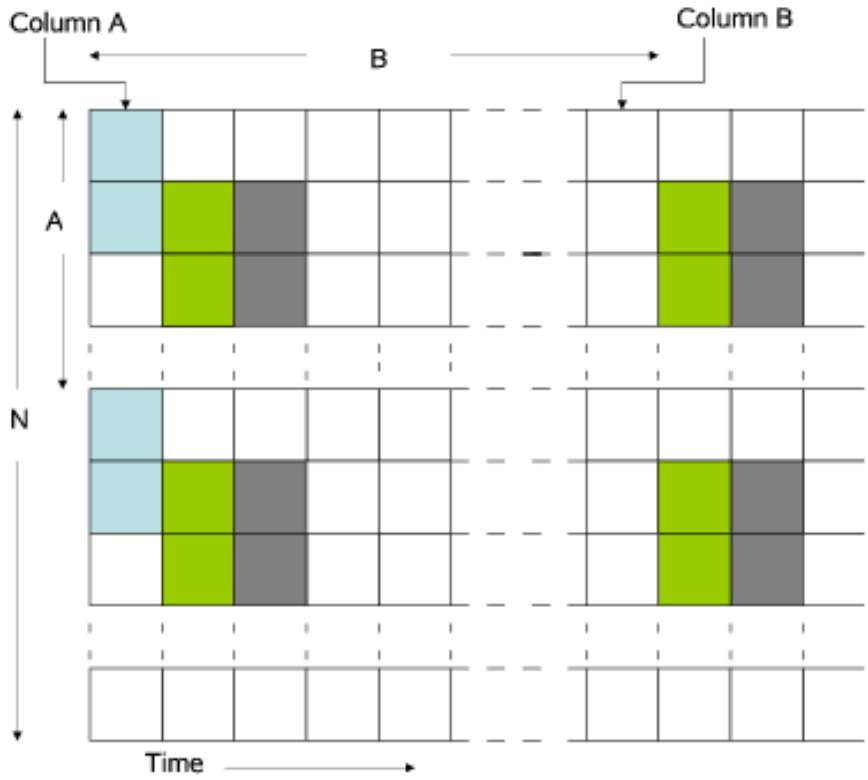

Figure 5.3.2:

in the Figire 5.3.2. is chosen in such a way that the basic operation can be done on the qubits in a translation invariant way in the horizontal axis and the modified qubits will be placed in the next column location, as shown in the Figure 5.3.2. the qubits are initially in the ColumnA location and after the operation they will be shifted to location ColumnB. Operations will be translation invariant on each column of the dual lattice and the logical qubits will be encoded in the form of electric qubits. Since this is a cellular automaton, the operations will be translation invariance with a particular period and the period will not depend of the size of the input.

The lattice diagram that is shown in the figure 5.3.2 is the dual lattice. Each pair of consecutive blue plaquette corresponds to a qubit each of which will be initially prepared in $|0\rangle$ state, consecutive green and grey pair of plaquette corresponds to the state $|H\rangle$ and $|S\rangle$ which are arranged periodically on code surface.

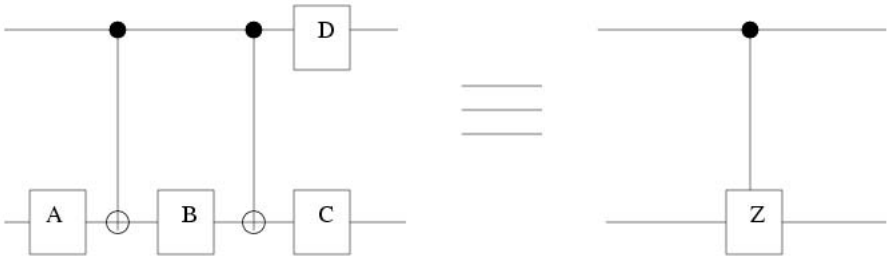

Figure 5.3.3: Equivalent circuit for $\Lambda(Z)_{1,2}$. Here $C = \exp(-i\frac{\pi}{2}Z)$, $B = \exp(i\frac{\pi}{4}Z)$, $A = \exp(i\frac{\pi}{4}Z)$ and $D = \exp(-i\frac{\pi}{4})\exp(-i\frac{\pi}{4}Z)$.

In this construction we will try to simulate the one-dimensional quantum cellular automaton described in [RR]. So the qubits encoded by the blue plaquette pairs corresponds to qubits present in the one-dimensional chain of [RR]. The operations that is done on the chain will be done to these qubits using the universal set of gates constructed earlier. The states $|A\rangle$ and $|Y\rangle$ are required to implement the gates $\exp(i\frac{\pi}{8}Z)$, $\exp(i\frac{\pi}{4}Z)$,$\exp(i\frac{\pi}{8}X)$.

The one-dimensional chain with N qubits in [RR] are initialized in the state $|00\ldots0\rangle$ and are repeatedly operated with the transition function

$$T = \left(\bigotimes_{i=1}^{N-1} \Lambda(Z)_{i,i+1}\right)\left(\bigotimes_{i=1}^{N} H_i\right). \tag{5.6}$$

In between the transitions one may apply translation invariant operations of the form

$$U_A(\alpha) = \bigotimes_{i=1}^{N} \exp\left(i\frac{\alpha}{2}A_i\right), \tag{5.7}$$

with A $\in \{X, Y, Z\}$. Each of the individual gates can be implemented with the universal set of gates that we have described earlier. For example $\Lambda(Z)_{1,2}$ that is used in the transition function T can be implemented using an alternative circuit given in Figure 5.3.3.

5.3.3 Fault Tolerance with Toric Code

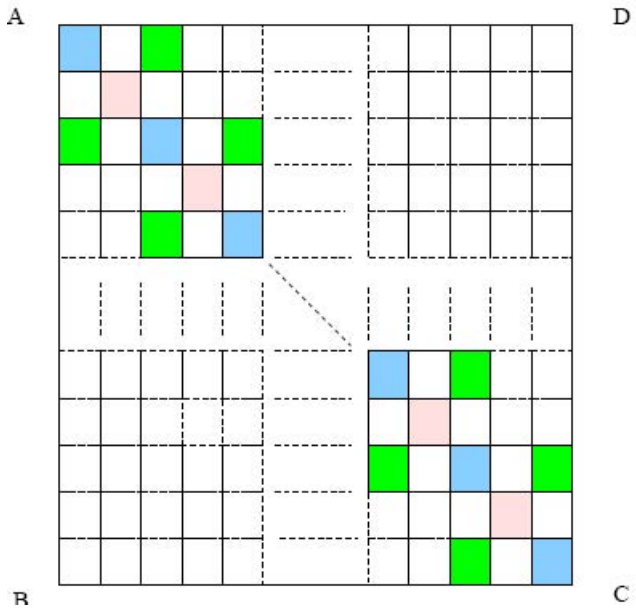

Figure 5.3.4: 2-dimensional quantum cellular automaton using surface codes.In this figure all the four edges AB, BC, CD, DA of surface code are rough edges.

Equivalent circuit for $\Lambda(Z)_{1,2}$. Here $C = \exp(-i\frac{\pi}{2}Z)$, $B = \exp(i\frac{\pi}{4}Z)$, $A = \exp(i\frac{\pi}{4}Z)$ and $D = \exp(-i\frac{\pi}{4})\exp(-i\frac{\pi}{4}Z)$.

Using the transition function defined in [RR] we will now build a cellular automaton on toric code. The code surface is divided in three types of cells, namely the *logical cell*, *distillation1 cell* , *distillation2 cell* , *connecting cell* and *computation cell*. The distillation cell 1 and 2 are used for the distillation of the states $|H\rangle$ and $|S\rangle$. In each distillation

cell two copies of $|H\rangle$ and $|S\rangle$ are distilled. The magic states formed in distillation1 cell are used for the computations and the ones produced in distillation1 cell will be used up for concatenation in the distillation1 cell. Connecting cells is a part of the surface code of same size size as the other cell with no surface defects, it is used for moving the magic states during distillation or for implementation of unitary gates on the logical bits. The logical cell is where the the logical qubits are placed, each cell contains one logical bit. The details of how the cells are arranged are shown in the Figure 5.3.4 and Figure 5.3.5.

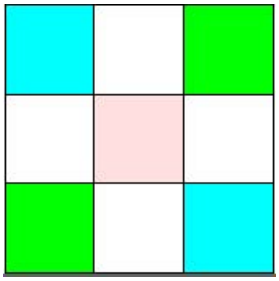

Figure 5.3.5: Diagram of the computational cell which is made up of two distillation2 cell (green), one distillation1 cell (pink), four connecting cells (white) and two unit cells (blue).

As in subsection **??** logical bits are encoded using a pair of electric defects. From the Figure 5.3.4 we can see that the computational cells are arranged in the diagonally on the surface code. The computational cell is big enough so that unitary gates can be applied to the logical qubits placed in the unit subcells using the magic states distilled from the distillation1 subcell of the computational cell. The *reset operation* is used to reset the structure of the unit as well as the distillation cells after an operations. The transition function and the transition invariant operations that is used is same as the ones that is used in [RR]. Those operation are implemented using CNOT, preparation/measurement X- and Z- eigen basis, $\exp(i\frac{\pi}{8}Z)$, $\exp(i\frac{\pi}{4}Z)$, $\exp(i\frac{\pi}{4}X)$. The later three can be implemented using the states $|H\rangle$ and $|S\rangle$.

Regarding the magic state distillation procedure: We here use procedures develop in [RJK] for the distillation of $|H\rangle$, $|S\rangle$ states. In each computational cell (Figure 5.3.5.) we see that there are two subcells of distillation2 type and one of distillation1 type. The scheme for concatenation of the distilled state for the next level of distillation is shown in Figure **??**. But the final distilled states are stored in distillation1 subcells which are used for the implementation of the unitary gates. After distillation is done the reset

operation is used to reset the cells other than the unit cells.

The appendix explains the Move operation and details of the implementation of magic state distillation.

5.4 Appendix A: Move operation

The Figure 5.4.6. shows the circuit to move the plaquette $P1$ to $P3$, where the two magnetic holes $P1$ and $P2$ encode a magnetic qubit. Here $Z(P3)$ belongs to the stabilizer set of the surface code.

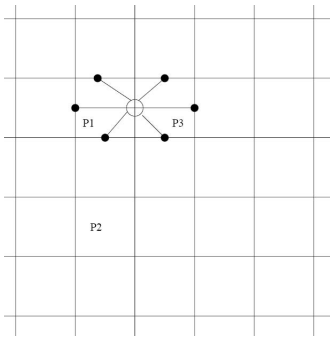

Figure 5.4.6: The circuit for moving magnetic holes on the code surface. The circuit will move the magnetic hole $P1$ to $P3$.

5.5 Appendix B: Universal computation by magic states

The theory of universal computation based on magic state distillation [KB05] assumes the fact that clifford gates , preparation of the state $|0\rangle$ and measuring eigenvalue of a Pauli operator on all the qubits can be implemented exactly. It can be shown that Clifford gates are sufficient for universal quantum computation if magic states (defined later) are also available. Lets consider a state

$$|A_\theta\rangle = 2^{-1/2}(|0\rangle + e^{i\theta}|1\rangle) \tag{5.8}$$

and suppose that θ is not a multiple of $\pi/2$. We now describe a procedure that implements the phase shift gate $\Lambda(e^{i\theta})$ by using Clifford gates and several copies of $|A_\theta\rangle$.

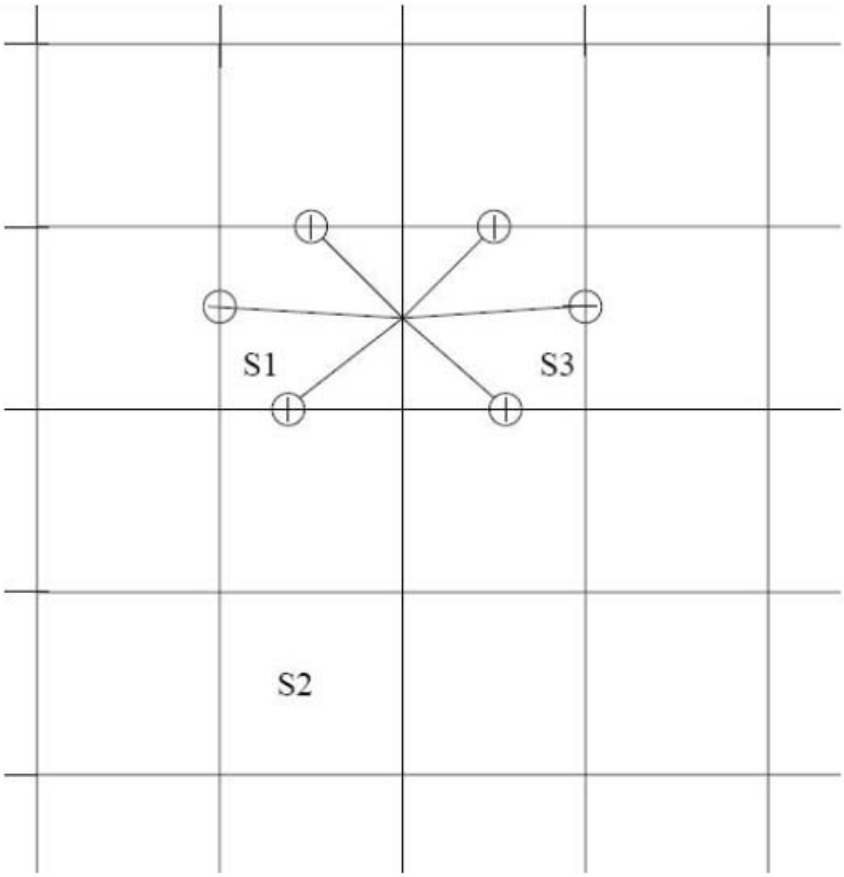

Figure 5.4.7: The circuit for moving electric holes on the dual code surface. The circuit will move the electric hole $S1$ to $S3$.

Let $|\phi\rangle = a|0\rangle + b|1\rangle$ be a state which must be acted upon by $\Lambda(e^{i\theta})$. Prepare the state $|\phi_0\rangle = |\phi\rangle \otimes |A_\theta\rangle$ and measure the stabilizer $S_1 = Z \otimes Z$. Note that both outcomes of this measurement come with probability 1/2. If the outcomes is '+1', we are left with the state

$$|\phi_1^+\rangle = (a|00\rangle + be^{i\theta}|11\rangle).$$

In the case of '-1' outcomes, the resulting state is

$$|\phi_1^-\rangle = (a|01\rangle + be^{i\theta}|10\rangle).$$

Let us apply CNOT gate ($\Lambda(X)$) by making the first qubit as the control and the second as the target. The result is

$$\begin{aligned} |\phi_2^+\rangle &= \Lambda(X)_{1,2}|\phi_1^+\rangle = (a|0\rangle + be^{e^{i\theta}}|1\rangle) \otimes |0\rangle, \\ |\phi_2^-\rangle &= \Lambda(X)_{1,2}|\phi_1^+\rangle = (ae^{i\theta}|0\rangle + b|1\rangle) \otimes |0\rangle. \end{aligned}$$

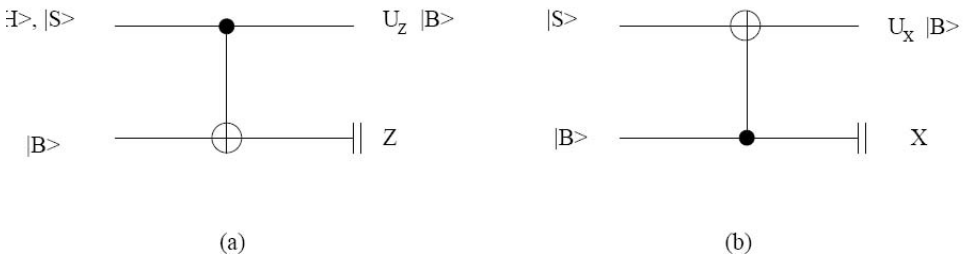

Figure 5.5.8: (a) Circuit for realization of $\exp(i\frac{\pi}{8}Z)$, $\exp(i\frac{\pi}{4}Z)$ gates using the sates $|H\rangle$, $|S\rangle$. (b) Circuit for the realization of $\exp(i\frac{\pi}{4}X)$ using $|S\rangle$.

The second qubit can be discarded to get the state $a|0\rangle + be^{\pm i\theta}|1\rangle$, depending on the measuring outcome. Applying the procedure repeatedly the we will get the unitary operations $\Lambda(e^{ip_1\theta}), \Lambda(e^{ip_2\theta}, \ldots$ for integers $p_1, p_2, \ldots$ which obey the random walk statistics. It is known that such random walks visits each integers with probability 1 and hence will visit 1. And the desired operator will be realized.

So now if we have a

$$\begin{aligned} |H\rangle &= \frac{(|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}} \\ &= |A_{-\pi/4}\rangle \end{aligned}$$

then one can realized the operator $\Lambda(e^{-i\pi/4})$.

The above idea of universal computation is used in [RJK] to get the gates $\exp(i\frac{\pi}{8}Z)$, $\exp(i\frac{\pi}{4}Z)$, $\exp(i\frac{\pi}{4}X)$ using the states $|H\rangle$ and $|S\rangle$.

References

[ADM] A. Mizel, D. A. Lidar, M. Mitchell, *Simple proof of the equivalence between adiabatic quantum computation and the circuit model*, quant-ph/0609067.

[AO06] A. Ambainis, Oded Regev, *An Elementary Proof of the Quantum Adiabatic Theorem*, arXiv:quant-ph/0411152, (2006).

[CS96] Calderbank and P. Shor, *Good quantum error-correcting codes exist*, Phys. Rev. A 54, 1098 (1996).

[Grover97] L. K. Grover *A Fast Quantum Mechanical Algorithm for Database Search*, quant-ph/9605043, Phys. Rev. Lett. 78,325 (1997).

[Fey82] R. P. Feynman, *Simulating Physics with Computers*, International Journal of Theoretical Physics, Vol. 21, pp 465-488 (1982).

[Fey96] R. P. Feynman, *Lectures on Computation*, A. J. G. Hey and R. W. Allen, editors, Addison Wesley (1996).

[MTW00] M. Mosca, A. Tapp, R. de Wolf, *Private Quantum Channels and the Cost of Randomizing Quantum Information*, eprint quant-ph/0003101 (2000).

[NC00] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[Messiah76] A. Messiah, *Quantum Mechanics*, Vol. II, Amsterdan: North Holland; New York: Wiley (1976).

[EJSM] E. Farhi, J. Goldstone, S. Guttmann, M. Sipser, *Quantum Computation by Adiabatic Evolution*, arXiv:quant-ph/0001106v1, (2000).

[NC] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Combridge University Press.

[JFS] S. P. Jordan, E. Farhi and P. Shor, *Error Correcting Codes For Adiabatic Quantum Computation*, arXiv:quant-ph/0512170.

[SS] S. Sachdev, *Quantum Phase Transition*, Cambridge University Press (1999).

[DA] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd and O. Regev, *Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation*, arXiv:quant-ph/0405098.

[CFP02] A. Childs, E. Farhi and J. Preskill, *Robustness of Adiabatic Quantum Computation*, *Physical Review A*, 65:012322,2002.

[D01] E. Dennis et al., *Topological Quantum Memory*, quant-ph/0110143 (2001).

[AL07] R. Alichi et al., *A statistical mechanics view on Kitaev's proposal for quantum memories*, arXiv:quant-ph/0702102 (2007).

[Kitaev03] A. Kitaev, *Fault-tolerant quantum computation by anyons Ann. Phys.* 303, 2(2003), arXiv:quant-ph/9707021 (2003).

[RJK] R. Raussendorf, J. Harrington and K. Goyal, *Topological fault-tolerance in cluster state quantum computation*, arXiv:quant-ph/0703143.

[KB] S. Bravyi and A. Kitaev, *Quantum codes on a lattice with boundary* ,arXiv:quant-ph/9811052.

[KB05] S. Bravyi and A. Kitaev,*Universal Quantum Computation with ideal Clifford gates and noisy ancillas*, *Phys. Rev. A* 71, 022316 (2005), arXiv:quant-ph/0403025 (2005).

[RR] R. Raussendorf,*Quantum computation via translation-invariant operations on a chain of qubits*, *Physical Review A* 72, 052301 (2005) arXiv:quant-ph/0505122 (2005).

[JED] J. Edmonds, Can. J. Math 17, 449(1965).

[JW95] J. Watrous, *On one-dimensional quantum cellular automaton*, in *Proceeding of the 36th IEEE Symposium on Foundation of Computer Science*,528 (1995).

[WVM96] W. v Dam, Master Thesis, University of Nijmegen (1996).

[Nielsen] M. A. Nielsen, *The Fermionic canonical commutation relations and the Jordan-Wigner transform.*

[GR07] Gernot Schaller and Ralf Schützhold, *The role of symmetries in adiabatic quantum algorihms*, quant-ph/0708.1882v1 (2007).

[M76] A. Messiah, *Quantum Mechanics*, Vol. 2, Amsterdam: North Holland; New York: Wiley (1976).

[ZG07] Z. Nussinov, G. Ortiz, *A symmetry principle for Topological Quantum Order*, arXiv:cond-mat/0702377.

[S97] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, *SIAM J. Comp.*, 26(5):1484-1509 (1997).

[S96] P. W. Shor, *Fault-tolerant quantum computation*. In *Proceedings, 37th Annual Symposium on Fundamentals of Computer Science*, pages 56-65, IEEE Press, Los Alamitos, CA (1996).