Chapter 1

Introduction and preliminaries

In the last 50 years, we have witnessed tremendous development in computer science. Moore's law asserts that the number of transistors that can be fabricated on an integrated circuit at a constant cost doubles approximately every two years. This rapid growth would only cease around 2020, where quantum mechanical effects dominate. While technologies are being explored to respond to this difficulty, there is one that regards this effect as a benefit: quantum information processing.

A quantum computer is different from traditional, *classical computers* in that it makes direct use of quantum mechanical features such as *superposition* and *entanglement* to perform operations on data encoded into quantum states. The basic principle behind quantum computation is *Feynman parallelism*, the ability to simultaneously follow multiple computational pathways. A theoretical model for this purpose is the *quantum Turing machine*, which generalizes the notion of *probabilistic Turing machine*. As a result, quantum computers can considerably outperform their classical counterparts for some class of problems.

In computational complexity theory an algorithm is efficient if the time (i.e., the number of steps) taken to solve the problem is a polynomial function of the size of the problem. Else (say, if the time is an exponential function of problem size), the algorithm is inefficient. An example of an algorithm, for which there is no known efficient algorithm on classical computer, but which can be efficiently implemented on quantum computers, is Shor's algorithm for finding the prime factors of an integer. Another example, where quantum computers offer a speed-up is Grover's algorithm for searching through an array of unsorted data of size N. Classically, $\mathcal{O}(N)$ queries are needed to search an unstructured data-base, while this can be reduced to $\mathcal{O}(\sqrt{N})$ if implemented quantum mechanically using Grover's algorithm. Also, simulating a quantum system is not in general, efficiently possible using classical computers. The composite state of n-qubits lives in a 2^n-dimensional space, so that an exponentially large number of classical registers (to

store the complex numbers corresponding to the amplitudes) are required to classically track the evolution of a quantum system of n qubits.

Because of nonclassical features like uncertainty, disturbance produced by quantum measurement and no-cloning, quantum protocols can be used to protect secret information, in the sense that the actions of an eavesdropper can be detected with non-zero probability. Quantum cryptography can provide unconditional security, unlike its classical counterpart, whose security depends on practical limitations, such as the computational complexity of a problem, based on known algorithms. For example, the security of RSA encryption hinges on the hardness of prime factorization, which is not known to be efficient on classical computers.

1.1 Basics of quantum mechanics

The fundamental unit of quantum information is the *qubit*, which could be any two-level quantum system. The levels are labeled as $|0\rangle$ and $|1\rangle$. A classical bit string can be described as a vector over the Galois field Z_2. Analogously, string of of n-qubits is a vector from Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ of dimension $d = 2^n$ over a field of complex numbers $\mathcal{C}$, where $\mathcal{H}_1, \ldots, \mathcal{H}_n$ represent the Hilbert space of individual qubits and "$\otimes$" is the tensor product. Accordingly, if $|0\rangle$ and $|1\rangle$ are the two possible states of a quantum system, then the linear combination

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.1}$$

is also a legitimate state where $\alpha, \beta \in \mathcal{C}$. This is known as principle of *superposition* in quantum mechanics. In general, pure state in an n-qubit system can be written as the superposition

$$|\Psi\rangle = \sum_{j=0}^{2^2-1} = \alpha_j|j_n\rangle, \tag{1.2}$$

where $|j_n\rangle$ is basis element for $\mathcal{H}$ and $\sum_{j=0}^{2^2-1} |\alpha_j|^2 = 1$.

Quantum entanglement A multi-particle superposition in which the state is not factorizable as a product of states of individual particles, is called entangelement. Entanglement can be harnessed to create quantum *parallelism* in a quantum computer, whereby one has a superposition of evaluation of all possible inputs x to a function $f(x)$, of the form:

$$2^{-n/2} \sum_x |x\rangle|0\rangle \rightarrow 2^{-n/2} \sum_j |x\rangle|f(x)\rangle. \tag{1.3}$$

Entanglement is a counter-intuitive feature of quantum mechanics, and one of the key ways in which quantum phenomena depart from classical mechanics. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be the two Hilbert spaces and let pure state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Then $|\psi\rangle$ is said to be disentangled or separable state if there exist states $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$ such that $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$; otherwise it is said to be entangled. Intuitively, entanglement is a fundamental resource of quantum information processing, though its exact power is still not fully understood.

There are two kinds of evolution in quantum mechanics: a discontinuous, probabilistic evolution following a measurement, and a continuous, norm-preserving (i.e., unitary) Schrödinger evolution

Measurement. Observables in quantum mechanics are represented by Hermitian operators. A measurement operator

$$\mathcal{O} = \sum_{j=0}^{2^n-1} \lambda_j |j_n\rangle\langle j_n|, \tag{1.4}$$

updates the the state $|\Psi\rangle$ to $|j_n\rangle$ with probability $|\langle j_n|\Psi\rangle|^2$. The corresponding measurement outcome is λ_j. To ensure that the probabilities of the possible outcomes sum to 1, projectors $|j_n\rangle\langle j_n|$ satisfy the completeness condition $\sum_{j=0}^{2^n-1} |j_n\rangle\langle j_n| = \mathbb{I}$. For example, after measurement in the $\{|0\rangle, |1\rangle\}$ basis, $|\psi\rangle$ collapses to either $|0\rangle$ or $|1\rangle$ with probability $|\alpha|^2 = |\langle 0|\psi\rangle|^2$ or $|\beta|^2 = |\langle 1|\psi\rangle|^2$, respectively. Thus follows the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. $|\alpha|^2$ and $|\beta|^2$ can be accessed by performing measurement on an ensemble of $|\psi\rangle$.

More generally, measurement can be represented by any partition of unit operator. This constitute a positive operator valued measurement (POVM). Unlike projectors POVM elements need not be idempotent matrix. A projector corresponding to a degenerate eigenvalue is sometimes called "incomplete", mainly in quantum error correction where syndrome measurements are such measurements.

Continuous evolution. The time evolution of a quantum state is determined by the Shr̈odinger equation

$$-i\hbar \frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle, \tag{1.5}$$

where H is the Hamiltonian of the system.

Density matrix representation

Quantum states can also be represented by $d \times d$ dimensional operators on Hilbert space $\mathcal{H}$ of dimension d known as density matrix. If $|\psi\rangle \in \mathcal{H}$ represents a quantum state, the

density matrix simply is

$$\rho = |\psi\rangle\langle\psi|, \tag{1.6}$$

where $\langle\psi|$ is from dual space corresponding to $\mathcal{H}$. From the properties of $|\psi\rangle$ it follows that $\rho \geq 0$ (positive semi-definite) and $\mathrm{Tr}(\rho) = 1$. The advantage of the density matrix representation over vector representation is that the former can represent any classical ensemble of *pure* states too.

An ensemble of pure states $\{p_k, |\psi_k\rangle\}$ with statistical weights p_k, is represented by density matrix

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|, \tag{1.7}$$

which is a convex combination of states as $p_k \geq 0$. From Eq. (1.6) and Eq. (1.7) it is observed that pure states are characterized by $\mathrm{Tr}(\rho^2) = 1$, whereas mixed states by $\mathrm{Tr}(\rho^2) < 1$. If $P_0 = |0\rangle\langle 0|$ is the projector corresponding to a measurement outcome $|0\rangle$, then the expectation value to obtain $|0\rangle$ in ρ is $\mathrm{Tr}(P_0\rho)$. In general if $\mathcal{O}$ is any quantum mechanical observable, represented by a Hermitian matrix, its expectation value in the state ρ is $\mathrm{Tr}(\mathcal{O}\rho) = \sum_k p_k \langle\psi_k|\mathcal{O}|\psi_k\rangle$.

Geometrically, the pure state of a qubit can be represented as a point on the three-dimensional sphere known as *Bloch* sphere, while the mixed states are points within the sphere. This can be seen by parameterizing the Eq. (1.1) with θ and ϕ as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{-i\phi}\sin\frac{\theta}{2}|1\rangle, \tag{1.8}$$

where the norm, $\cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} = 1$, represents the surface of sphere with unit radius. The density matrix of a qubit in the Pauli operator basis is

$$\rho = \frac{I_2 + \hat{n}\cdot\sigma}{2}, \tag{1.9}$$

where $\hat{n} = \{\hat{n}_x, \hat{n}_y, \hat{n}_z\}$, $\sigma = \{\sigma_x, \sigma_y, \sigma_z\}$ and I_2 is the 2×2 identity matrix. The Bloch vector $\hat{n}$ is simply the expectation value of ρ in the Pauli basis, i.e., $\hat{n} \equiv (\langle\sigma_x\rangle, \langle\sigma_y\rangle, \langle\sigma_z\rangle)$. The Pauli operators are traceless and have representation in the computational basis as

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.10}$$

The computational basis vectors $\{|0\rangle, |1\rangle\}$ are eigenvectors of σ_z. From Eq. (1.9) $\mathrm{Tr}(\rho^2) = 1$ corresponds to $\hat{n}_x^2 + \hat{n}_y^2 + \hat{n}_z^2 = 1$ which represents the surface of Bloch sphere. Also it can be verified that for mixed states $\mathrm{Tr}(\rho^2) = \hat{n}_x^2 + \hat{n}_y^2 + \hat{n}_z^2 < 1$ which represent the interior of the Bloch sphere. The *completely* mixed state $\rho = I_2/2$ is the center of the

Bloch sphere which represents an equal mixture of $|0\rangle$ and $|1\rangle$.

Operations on quantum states

Operations required for quantum information processing are known as gates, which are unitary operations, mathematically represented by unitary matrices U, that satisfy $UU^\dagger = U^\dagger U = I$. The U transforms initial state of the quantum computer to the required final state $|\psi'\rangle$,

$$|\psi'\rangle = U|\psi\rangle, \tag{1.11}$$

which can be read by performing measurement. One can observe that the $\langle\psi'|\psi'\rangle = 1$ and thus U is trace preserving operation. This evolution corresponds to that described by Eq. (1.5), where $U = e^{-iHt/\hbar}$. The Pauli operators are unitary and can perform various required operations on quantum computers. The basic gates used in quantum computation are bit-flip (σ_x), phase-flip (σ_z), combination bit and phase flips ($\sigma_y = \sigma_x\sigma_z$), Hadamard and controlled NOT (CNOT). Hadamard gate does a $\frac{\pi}{4}$-rotation on the qubit space. CNOT is a two-qubit gate that flips the second qubit conditioned on the state of the first qubit: $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$. Using a CNOT and a $SU(2)$ gate, any unitary quantum operation on qubits can be simulated and hence they form a universal set of gates for quantum computation.

In general, the gates on qubits and qubits themselves would be noisy due their unavoidable interaction with the surrounding and leads to non-unitary evolution. This would be described in detail in the following Sec 1.2.

1.2 Quantum noise

The chief barrier in realizing the quantum computation, apart from the difficulty to scale-up, is that a quantum system is rarely truly isolated: it tends to interact with its environment (also substituted by words bath and reservoir) and is thus usually *open*. These interactions are often unwanted (though exceptions exist [1]) and difficult-to-eliminate. They show up as *noise* in quantum information processing systems and *decoheres* the system. Decoherence causes decay of the quantum information about the coherence in the system in a basis determined by the interaction Hamiltonian [2], which could be the position basis or the eigen basis of the system Hamiltonian, leading to familiar classical behavior. One of the first testing grounds for open system ideas was in quantum optics [3]. Its application to other areas gained momentum from the works of Caldeira and Leggett [4], and Zurek [5], among others.

Depending on its nature, the system-environment interaction can be classified as *dissi-*

pative or *quantum non-dissipative*. When the system Hamiltonian H_S does not commute with the interaction Hamiltonian H_{SR}, the resulting interaction is dissipative, giving rise to dissipation of energy where the population of the system changes. This class of interaction results in *amplitude damping* along with *dephasing*. When H_S and H_{SR} commute, the class of interactions is energy-preserving and only dephasing occurs without amplitude damping and are known as quantum non-dissipative interactions [6]. This type of noise has no classical analogue. Amplitude damping channels are of the former kind, while the phase flip channel is of the latter kind.

Quantum operations

A quantum operation, also called quantum map, $\mathcal{E}$ describes the evolution of one quantum state ρ to another $\rho' = \mathcal{E}(\rho)$. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ denote the input and output spaces of $\mathcal{E}$. Let $B(\mathcal{H}_1)$ and $B(\mathcal{H}_2)$ denote the set of density operators acting on $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively. A mapping $\mathcal{E}$ from $B(\mathcal{H}_1)$ to $B(\mathcal{H}_2)$ is quantum operation if it satisfies the following conditions:

1. linear
2. trace non-increasing, i.e., $\mathrm{tr}(\mathcal{E}(\rho)) \leq \mathrm{tr}(\rho)$ for all $\rho \geq 0$
3. *completely positive* (CP) [7].

A mapping is called positive if $\rho \geq 0$ in $B(H_1)$ implies $\mathcal{E}(\rho) \geq 0$ in $B(H_2)$. It is called completely positive if, for any auxiliary Hilbert space H_a, $\forall\ \tilde{\rho} \geq 0$ in $B(\mathcal{H}_1 \otimes \mathcal{H}_\mathrm{a})$ implies $(\mathcal{E} \otimes I_\mathrm{a})\tilde{\rho} \geq 0$ in $B(\mathcal{H}_2 \otimes \mathcal{H}_\mathrm{a})$, where I_a is identity operator in $B(\mathcal{H}_\mathrm{a})$.

Every completely positive map $\mathcal{E}$ has Kraus or operator sum representation [8, 9],

$$\mathcal{E}(\rho) = \sum_j K_j \rho K_j^\dagger, \tag{1.12}$$

where $\sum_j K_j^\dagger K_j \leq \mathbb{I}$ and $\mathbb{I}$ is the identity operator in $\mathcal{H}_1$. K_j are called Kraus operators or operation elements of $\mathcal{E}$. This provides a convenient representation useful in quantum information theory, especially in quantum error correction. However, constructing Kraus representation for CP map whose corresponding Choi matrix is not analytically diagonalizable is not possible [10]. This impasse is dealt in detail in the Chapter 4 of the thesis. Complete positivity requirement ensures that if the input is entangled with some other system, the output state will be a valid quantum state.

The quantum operation can be realized physically in the following way:

$$\mathcal{E} = \mathrm{Tr}_\mathrm{o}[U(\rho \otimes \rho_\mathrm{a})U^\dagger(I \otimes P_\mathrm{o})], \tag{1.13}$$

where $\rho_{\rm a} \in B(\mathcal{H}_{\rm a})$ is the density matrix of the initial state of ancilla, $\mathbb{I} \in B(\mathcal{H}_2)$ is identity operator, $\mathcal{H}_1 \otimes \mathcal{H}_{\rm a}$ and $\mathcal{H}_2 \otimes \mathcal{H}_{\rm o}$ are the input and output spaces of the composite system respectively, $P_{\rm o} \in B(\mathcal{H}_{\rm o})$ is a projector. $\mathrm{Tr}_{\rm o}$ represents tracing over the Hilbert space $\mathcal{H}_{\rm o}$. This approach describes the system environment (ancilla) interaction. Each of these evolutions result from unitary interaction of the system with a fixed state of an ancilla $\rho_{\rm a}$, followed by measurement on subsystem $\mathcal{H}_{\rm o}$ with measurement operators $[P_o, I - P_{\rm o}]$, post-selection on the first outcome, and removing $\mathcal{H}_{\rm o}$.

Quantum maps $\mathcal{E}$ are also interchangeably called as quantum channels. Some familiar noise channels are the depolarizing channel, the dephasing channel, the amplitude damping channel and generalized amplitude damping channel [11, 12]. A generalization of the latter, in which the thermal bath is squeezed, known as squeezed generalized amplitude damping channel was introduced in Ref. [13].

1.2.1 Markovian master equation

Tools other than quantum operations can be employed in studying the open quantum systems. One of them is the Lindblad-Gorini-Kossakowski-Sudarshan (LGKS) *master equation* [14, 15], a picture of quantum noise complementary to the quantum operations formalism. The main objective here is to describe the time evolution of the open quantum system with a differential equation which describes the non-unitary behavior. It is assumed here that the system and environment start out in an initially product state. If the system and environment are initially correlated, then the above formalisms break down, and in general the evolution can no longer be represented as a CP map [16, 17]. The general form of *master equation* is

$$\frac{d}{dt}\rho(t) = \mathcal{L}\rho(t). \tag{1.14}$$

As the Hamiltonian H generates the unitary operator for time evolution of a closed system, the linear operator $\mathcal{L}$ generates a finite super-operator, called *Lindbladian*, that takes into consideration non-unitary evolution due to open quantum system effects. The general solution for the above equation is

$$\rho(t) = e^{\mathcal{L}t}\rho(0). \tag{1.15}$$

If the $\mathcal{L}$ is time independent, Eq. (1.15) describes Markovian evolution which is quantum dynamical semigroup with single parameter $t \geq 0$. The resulting channel is memoryless, i.e., the evolution of the state depends only on the instant state $\rho(t)$, not on its history.

The Markovian master equation can be cast into the following form [14, 15]

$$\frac{d}{dt}\rho(t) = \mathcal{L}\rho(t) = -i[\mathcal{H}, \rho(t)] + \sum_{\mu}\left(L_\mu \rho(t) L_\mu^\dagger - \frac{1}{2}L_\mu^\dagger L_\mu \rho(t) - \frac{1}{2}\rho(t) L_\mu^\dagger L_\mu\right), \quad (1.16)$$

and is guaranteed to be completely positive. The first term in the equation is the usual Schrödinger term that generates unitary evolution. The other terms describe the possible transitions the system may under go due to interaction with the environment, which are non-unitary in nature. The L_μ's are called *Lindblad* or *quantum jump* operators.

1.2.2 Interaction with a squeezed thermal bath

Upon quantization the x-component of electric and magnetic field operators can be written as [18]

$$\begin{aligned} E_x &= \sqrt{\frac{\hbar\omega}{\epsilon_0 V}}(be^{-i\omega t} + b^\dagger e^{i\omega t})\sin(kz) \\ iB_x &= \sqrt{\frac{\hbar\omega}{\epsilon_0 V}}(be^{-i\omega t} - b^\dagger e^{i\omega t})\cos(kz), \end{aligned} \quad (1.17)$$

where the fields propagate along z-axis, V corresponds to the enclosing volume and b and $b^\dagger$ are field annihilation and creation operators respectively satisfying the commutation relation $[b, b^\dagger] = 1$. The quadreture operators for the field are defined as

$$\begin{aligned} Q_1 &= \frac{1}{2}(b + b^\dagger) \\ Q_2 &= \frac{1}{2i}(b - b^\dagger), \end{aligned} \quad (1.18)$$

and satisfy $[Q_1, Q_2] = i/2$. The electric field operator written in terms of quadrature operators is

$$E_x = 2\sqrt{\frac{\hbar\omega}{\epsilon_0 V}}\sin(kz)\left[Q_1\cos(\omega t) + Q_2\sin(\omega t)\right]. \quad (1.19)$$

It can be noted from he above expression that Q_1 and Q_2 correspond to amplitude of the field oscillating with a phase difference of $\pi/2$ betweem the quadratures.

In the *coherent* states,

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n}}|n\rangle, \quad (1.20)$$

where $|n\rangle$ is number state (eigenstate of the number operator $b^\dagger b$), fluctuations in the two quadratures are equal and minimize the uncertainty product given by Heisenberg's uncertainty principle:

$$\langle(\triangle Q_1)^2\rangle = \langle(\triangle Q_2)^2\rangle = \frac{1}{4} \quad (1.21)$$

The fluctuations in coherent states are equal to *zero-point* fluctuations and are distributed randomly in phase. The zero-point fluctuation represent the standard quantum limit to the reduction of noise (uncertainty) in a signal. It is however possible to generate the states which have lesser fluctuation in one quadrature than a coherent state, at the expense of increased fluctuation in the other quadrature. Such states are called *squeezed* states.

Mathematically squeezed states are obtained by applying the squeezing operator

$$\mathbb{S}(s_k, \Phi_k) = \exp\left[\frac{s_k}{2}\left(b_k^{\dagger 2} e^{-i2\Phi_k} - b_k^2 e^{i2\Phi_k}\right)\right], \tag{1.22}$$

where s_k, Φ_k are the squeezing parameters on the states. Consider the action of $\mathbb{S}(s_k, \Phi_k)$ on vacuum state $|0\rangle$. We find that for the squeezed vacuum state

$$\begin{aligned}
\langle(\triangle Q_1)^2\rangle &= \frac{1}{4}\left[\cosh^2(s_k) + \sinh^2(s_k) - 2\cosh(s_k)\sinh(s_k)\sin\Phi_k\right], \\
\langle(\triangle Q_2)^2\rangle &= \frac{1}{4}\left[\cosh^2(s_k) + \sinh^2(s_k) + 2\cosh(s_k)\sinh(s_k)\sin\Phi_k\right].
\end{aligned} \tag{1.23}$$

For $\Phi_k = 0$ this reduces to,

$$\begin{aligned}
\langle(\triangle Q_1)^2\rangle &= \frac{1}{4}e^{-2s_k} \\
\langle(\triangle Q_2)^2\rangle &= \frac{1}{4}e^{2s_k}.
\end{aligned} \tag{1.24}$$

From the above relation it can be seen that for the squeezed states, the fluction in a quadrature can be reduced below that for coherent states by increasing the parameter s_k.

The bath consisting of spin variables or harmonic oscillators that start in a squeezed state, is known as *squeezed bath*. Noise due to interaction with a squeezed bath has been studied via the master equation approach for a single qubit [13] and multi-qubit cases [19]. The quantum non-dissipation dynamics of a single qubit [20] and multiple qubits [21] have been studied. Squeezing of the environment introduces new features that are absent in open quantum systems. In particular, in certain regimes, squeezing counteracts the effect of thermal effects, causing a state to decohere at a slower rate, leading to preservation of quantum information encoded in it [20, 22, 23], which is advantageous in quantum information processing.

The squeezed thermal bath can be mathematically obtained by applying the squeezing operator $\mathbb{S}(s_k, \Phi_k)$ on the density matrix corresponding to a thermal bath

$$\rho_{\mathrm{R}}^{\mathrm{th}} = \Pi_k \left(1 - e^{-\frac{\hbar\omega_k}{k_B T}}\right) e^{-\frac{\hbar\omega_k}{k_B T} b_k^\dagger b_k}, \tag{1.25}$$

where b_k and $b_k^\dagger$ are the annihilation and creation operators, respectively corresponding to the kth mode of the bath. The squeezed thermal state of a reservoir is

$$\rho_{\rm R}^{\rm sqth} = \mathbb{S}(s_k, \Phi_k)\rho_{\rm R}^{\rm th}\mathbb{S}(s_k, \Phi_k)^\dagger. \tag{1.26}$$

Here are some physical environments that are engineered to produce squeezed reservoir (cf. [13]). To model a squeezed reservoir, one may use an infinite array of beam-splitters [24]. The signal is input from the left of the array. The output of each beam-splitter is input into the subsequent one, with identical and independent squeezed light input into the other port. The squeezed reserviour is realized in the limit of infinite number of beam-splitters. In Ref.([25]), J. F. Poyatos, J. I. Cirac and P. Zoller implemented quantum reservoir engineering with laser-cooled trapped ions in order to mimic the dynamics of an atom set in a squeezed vacuum reserviour. In Ref.([26]) a method of bath engineering to realized squeezed reserviour where the qubit is given by the two ground levels of an atom connected by an angular momentum transition driven by weak laser fields and coupled to a vacuum bath was presented. The reserviour is realized in optical pumping via the interference between the channels of spontaneous emission. The thus engineered bath parameters are controlled through the laser parameters.

Dissipative interaction

Consider a system of n-qubits (say, array of n two-level atoms) interacting with a reservoir modelled as 3-D electromagnetic waves. The total Hamiltonian describing the reservoir, system and the dissipative dipole interaction between them has the form [27]

$$\begin{aligned} H &= H_{\rm S} + H_{\rm B} + H_{\rm SR} = \sum_i^n \hbar\omega_i\sigma_i^z + \sum_{\vec{k}_p} \hbar\omega_k(b_{\vec{k}_p}^\dagger b_{\vec{k}_p} + 1/2) \\ &\quad - i\hbar\sum_{k_p}\sum_i^n \vec{\mu}_i.\vec{g}_{\vec{k}_p}(\vec{r}_i)(\sigma_i^+ + \sigma_i^-)b_{\vec{k}_p} - \text{h.c}, \end{aligned} \tag{1.27}$$

where $\vec{\mu}_i$ are the atomic dipole moments depending on the positions r_i of the qubits and σ_i^+, σ_i^- are the rising and lowering operators on the ith qubit. ω_i is the resonant frequency corresponding to the energy difference between the two levels of ith qubit. $b_{\vec{k}_p}^\dagger, b_{\vec{k}_p}$ are creation and annihilation operators of bath mode $\vec{k}_p$ corresponding to wave vector $\vec{k}$, frequency ω_k and polarization index $p = 1, 2$. Note that $[H_{\rm S}, H_{\rm SR}] \neq 0$, which is the signature of dissipative interaction. The system-reservoir coupling has the form

$$\vec{g}_{\vec{k}_p}(\vec{r}_i) = \sqrt{\frac{\omega_k}{2\epsilon\hbar V}}\vec{e}_{\vec{k}_p}e^{\vec{k}_p.r_i} \tag{1.28}$$

where $\vec{e}_{\vec{k}_p}$ is the unit polarization vector of the reservoir mode and V is the normalization volume.

The interaction Hamiltonian, $H_{\rm SR}$, in the interaction picture [6] is

$$\begin{aligned} H^{\rm I}(t) &= e^{-iH_0t/\hbar}H_{\rm SR}e^{iH_0t/\hbar} \\ &= \sum_{ks}\sum_{i}\vec{\mu}_i.\vec{g}_{\vec{k}_p}(\vec{r}_i)\sigma_i^+ b_{\vec{k}_p}e^{-i(\omega_k-\omega_i)t} + \vec{\mu}_i.\vec{g}_{\vec{k}_p}(\vec{r}_i)\sigma_i^- b_{\vec{k}_p}e^{-i(\omega_k+\omega_i)t} - \text{h.c} \quad (1.29) \end{aligned}$$

According to rotating wave approximation, terms like $2\omega_i, \omega_i+\omega_j$ oscillating at higher frequencies in $H^{\rm I}(t)$ are ignored. Subsequently, by tracing out the bath degrees of freedom, the reduced dynamics of the system under the Born-Markov rotating wave approximation in the weak coupling limit is determined by [27]

$$\begin{aligned} \frac{\partial}{\partial t}\rho &= -i\sum_i \omega_i\sigma_i^z\rho + i\sum_i \omega_i\rho\sigma_i^z - i\sum_{i,j}\Omega_{ij}\sigma_i^+\sigma_j^-\rho + i\sum_{i,j}\Omega_{ij}\rho\sigma_i^+\sigma_j^- \\ &- \frac{1}{2}\sum_{i,j=1}\Gamma_{ij}[1+\tilde{N}](\rho\sigma_i^+\sigma_j^- + \sigma_i^+\sigma_j^-\rho - 2\sigma_j^-\rho\sigma_i^+) \\ &- \frac{1}{2}\sum_{i,j=1}\Gamma_{ij}\tilde{N}(\rho\sigma_i^-\sigma_j^+ + \sigma_i^-\sigma_j^+\rho - 2\sigma_j^+\rho\sigma_i^-) + \frac{1}{2}\sum_{i,j=1}\Gamma_{ij}\tilde{M}(\rho\sigma_i^+\sigma_j^+ + \sigma_i^+\sigma_j^+\rho - 2\sigma_j^+\rho\sigma_i^+) \\ &+ \frac{1}{2}\sum_{i,j=1}\Gamma_{ij}\tilde{M}^*(\rho\sigma_i^-\sigma_j^- + \sigma_i^-\sigma_j^-\rho - 2\sigma_j^-\rho\sigma_i^-). \quad (1.30) \end{aligned}$$

In Eq.(1.30),

$$\begin{aligned} \tilde{N} &= N_{\rm th}\left(\cosh^2 s + \sinh^2 s\right) + \sinh^2 s, \\ \tilde{M} &= -\frac{1}{2}\sinh(2s)\,(2N_{\rm th}+1)\,e^{i\Phi}, \quad (1.31) \end{aligned}$$

where $N_{\rm th} = 1/(e^{\frac{\hbar\omega}{k_BT}}-1)$ is the Plank distribution. $\tilde{N}$ and $\tilde{M}$ characterize the squeezing in the bath, such that $\tilde{N}$ is the number of photons in the mode $\vec{k}_p$ and $\tilde{M}$ is two-photon correlations between the bath modes and Φ is the squeezing angle. In Eq.(1.30) Ω_{ij} represents the collective coherent effect due to multi qubit dissipative interaction with the bath and is given by

$$\Omega_{ij} = \frac{3}{4}\sqrt{\Gamma_i\Gamma_j}\left[-[1-(\hat{\mu}.\hat{r}_{ij})^2]\frac{\cos(k_0r_{ij})}{k_0r_{ij}} + [1-3(\hat{\mu}.\hat{r}_{ij})^2]\,[\frac{\sin(k_0r_{ij})}{(k_0r_{ij})^2} + \frac{\cos(k_0r_{ij})}{(k_0r_{ij})^3}]\right] \quad (1.32)$$

where $\Gamma_i = \frac{\omega_i^3\mu_i^2}{3\pi\varepsilon\hbar c^3}$ is the spontaneous emission rate corresponding to single qubit dissipative interaction. The term Γ_{ij} represents the collective incoherent effect due to multi

qubit dissipative interaction with the bath and is given by

$$\Gamma_{ij} = \frac{3}{2}\sqrt{\Gamma_i\Gamma_j}\left[[1-(\hat{\mu}.\hat{r}_{ij})^2]\frac{\sin(k_0 r_{ij})}{k_0 r_{ij}} + [1-3(\hat{\mu}.\hat{r}_{ij})^2]\left(\frac{\cos(k_0 r_{ij})}{(k_0 r_{ij})^2} - \frac{\sin(k_0 r_{ij})}{(k_0 r_{ij})^3}\right)\right]. \tag{1.33}$$

In the Eq.(1.32) and Eq.(1.33) $\hat{\mu}$ and $\hat{r}_{ij}$ are the unit vectors along the dipole moment and $\vec{r}_{ij}$ respectively where as $k_0 = \omega_0/c$ and $r_{ij} = |\vec{r}_{ij}|$.

Non-dissipative interaction

Consider the Hamiltonian describing the evolution of the total system

$$H = H_{\rm S} + H_{\rm S} + H_{\rm SR} = \sum_i^n \hbar\omega_i\sigma_i^z + \sum_{\vec{k}_p}\hbar\omega_k(b^\dagger_{\vec{k}_p}b_{\vec{k}_p}) - i\hbar\sum_{\vec{k}_p}\sum_i^n \sigma_i^z\left(\vec{g}_{\vec{k}_p}(\vec{r}_i)b^\dagger_{\vec{k}_p} + \vec{g}^*_{\vec{k}_p}(\vec{r}_i)b_{\vec{k}_p}\right), \tag{1.34}$$

where apparently $[H_S, H_{SR}] = 0$. Hence the resulting dynamics is non-dissipative in nature. Following the approximations, we have the dynamics of the reduces system described by [20]

$$\frac{d}{dt}\rho^{nm}(t) = \left[-\frac{i}{\hbar}(\epsilon_n - \epsilon_m) + i\dot{\eta}(t)(\epsilon_n^2 - \epsilon_m^2) - (\epsilon_n - \epsilon_m)^2\dot{\gamma}(t)\right]\rho^{nm}(t), \tag{1.35}$$

where

$$\begin{aligned}\eta(t) &= -\sum_k \frac{g_k^2}{\hbar^2\omega_k^2}\sin(\omega_k t),\\ \gamma(t) &= \frac{1}{2}\sum_k \frac{g_k^2}{\hbar^2\omega_k^2}\coth\left(\frac{\beta\hbar\omega_k}{2}\right)\left|(e^{i\omega_k t}-1)\cosh(r_k) + (e^{-i\omega_k t}-1)\sinh(r_k)e^{2i\Phi_k}\right|^2.\end{aligned} \tag{1.36}$$

$\beta = 1/k_B T$, k_B being the Boltzmann constant. For the case of zero squeezing, $r = \Phi = 0$, and $\gamma(t)$ given above reduces to the expression obtained for the case of a thermal bath [28, 29, 30]. It can be seen that $\eta(t)$ is independent of the bath initial conditions and hence remains the same as for the thermal bath. Note that in Eq. (1.35), the term responsible for the decay of coherences, i.e., the coefficient of $\dot{\gamma}(t)$ is dependent on the eigenvalues ϵ_n of the 'conserved pointer observable' operator which in this case is the system Hamiltonian itself. This reiterates the observation that the decay of coherence in a system interacting with its bath via non-dissipative interaction depends on the conserved pointer observable and the bath coupling parameters [29].

In the both, dissipative and non-dissipative cases the wave vector $k_0 = \frac{2\pi}{\lambda_0}$, where λ_0 is the resonant wave length, sets the length scale in to the problem depending upon the

ratio $\frac{r_{ij}}{\lambda_0}$. The dynamics of decoherence of the qubit system due to interaction with the bath can be classified as collective and independent decoherence model depending on $\frac{r_{ij}}{\lambda_0}$. When $\frac{r_{ij}}{\lambda_0} \to 0$, we obtain the collective decoherence model where as $\frac{r_{ij}}{\lambda_0} \geq 1$ gives rise to independent decoherence model.

1.3 Quantum error correction

Fragile, but very essential for quantum computation, the quantum superposition and entanglement in quantum systems decay due to quantum noise arising from interactions with the surrounding. Due to noise, like the analogue Turing machine, quantum Turing machine too would be inefficient. Fortunately, the emergence of the theory of quantum error correction and fault tolerant quantum computation offers hope here.

Quantum error correction was discovered independently by Shor and Steane. In Ref. [31] Shor introduced the 9-qubit quantum error correcting (QEC) code that encoded a qubit and could correct an arbitrary single-qubit error in the independent error limit i.e., the errors on different qubits are not statistically correlated. Calderbank and Shor [32], and Steane[33] independently developed CSS class codes (named after the inventors) that encodes a qubit in 7-qubits, for correcting arbitrary independent single-qubit errors using the ideas from classical error correction theory. The conditions on performing quantum error correction was introduced independently by Bennett, Divincenzo, Smolin and Wooters [34] and by Knill and Laflame [35], based on the work by Ekert and Macchiavello [36]. The 5-qubit QEC was discovered by Bennett, Divincenzo, Smolin and Wooters [34] and also independently by Laflame, Miquel, Paz and Zurek [37]. This encodes one qubit in five qubits and corrects arbitrary independent single-qubit errors. A stabilizer description of QEC codes was introduced by Gottesman [38, 39]. In this method, attention is given to operators rather than on code words (the encoding states).

Correlated errors. In Ref. [40], collective decoherence giving rise to correlated errors due to quantum non-demolition (QND) interaction on a n-qubit register was considered. In the noise model there, spatial correlation in the decoherence was controlled by varying the inter-qubit distance in the register and was described by the correlation matrix method. By applying the conventional single-error correcting schemes the performance of codes, evaluated via fidelity, against such noise was studied. It was found that such QEC schemes reduce the correlated decoherence. The action of correlated errors on CSS codes was considered by Klesse et al. [41], who showed quantitatively how error correlations have adverse effect on the performance of CSS codes. Ref. [42] considered correlated 'semi-classical' (i.e., parametric) noise described by a set of Gaussian random variables.

Degenerate codes The idea of degenerate codes, where the more than one error take a QEC code to same state and thus share the same recovery operation, was discovered by Shor and Smolin [43]. Ref. [44] provided a heuristic to construct degenerate codes for Pauli channels. In Ref. [45], the Hamming bound in the presence of degeneracy is discussed for the codes. A degenerate version of Hamming bound was provided in [46] and showed that the codes work against correlated errors by violating the usual Hamming bound.

Approximate error correcting codes Some times, constructing channel specific QEC codes would result in better performance against noise. Such codes were introduced in Ref. [47] for amplitude damping error. In Ref. [48] it was shown that it is possible to have approximate quantum error correcting codes for the channels that decrease the coherent information by a small ammount. The error correcting conditions for QEC codes were generalised to suit the approximate quantum error correction in Refs. [49, 50].

1.3.1 Basics

The basic idea behind the QEC is embed a smaller dimensional space in a larger one, such that the added redundancy gives protection against noise. There is a suitable error operator basis, such that errors here shift the code space to mutually orthogonal subspaces in the larger dimensional space. This ensures that the errors can be detected and corrected by devising suitable measurements and recovery operations. The basic ideas of the QEC can be illustrated by the following example.

3-qubit bit-flip code

The 3-qubit bit-flip code is similar to a repetition code used in classical error correction where the bits "0" and "1" are encoded as, $0 \rightarrow 000$; $1 \rightarrow 111$. Classically, the only possible error is bit-flip. Recovery from error consists in outputting 0 or 1, depending on the majority of 0's and 1's. However, it is apparent that the scheme decodes wrongly if the flip happens on two or more bits. If the probability of a bit flip is p, the probability that two or more bits are flipped is $p_f = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$ (probability of failure). The encoding is useful if $p_f < p$, which happens when $p < 1/2$.

When trying to mimic the classical repetition to construct QEC codes for a qubit, one faces the following difficulties:

1. A arbitrary quantum cannot be repeated, due to the *no cloning theorem.*

2. Measurement performed on qubits destroys the state.

3. A continuum of errors is possible on qubits unlike just bit flip on classical states.

The above mentioned difficulties are surpassed by encoding a qubit $|\psi\rangle$ as

$$|\psi_L\rangle \equiv \alpha|000\rangle + \beta|111\rangle, \tag{1.37}$$

where the encodings are of the form

$$|0\rangle \longrightarrow |0_L\rangle \equiv |000\rangle; \quad |1\rangle \longrightarrow |1_L\rangle \equiv |111\rangle. \tag{1.38}$$

Note that the encoding, Eq. (1.37) is not a repetation of state $|\psi\rangle$. Also, error detection should not reveal any information about $|\psi_L\rangle$. If a bit-flip error happens on one of the three qubits of the $|\psi_L\rangle$, it can be detected and corrected using the following two steps.

Error detection. To detect errors, a set of a set of measurement is to be performed on the QECC. The measurement result is called *error syndrome*. For a bit-flip channel there are four error syndromes corresponding to following four mutually commuting measurement operators:

$$\begin{aligned} P_1 &= |000\rangle\langle 000| + |111\rangle\langle 111|, \\ P_2 &= |100\rangle\langle 100| + |011\rangle\langle 011|, \\ P_3 &= |010\rangle\langle 010| + |101\rangle\langle 111|, \\ P_4 &= |001\rangle\langle 001| + |110\rangle\langle 110|. \end{aligned} \tag{1.39}$$

Since P_1, P_2, P_3, P_4 are mutually commuting, the operator $\hat{S} = \alpha P_1 + \beta P_2 + \gamma P_3 + \delta P_4$, where the coefficients are some real numbers, can be used for syndrome measurement. If the outcome of $\hat{S}$ is α, then no error occurred on qubits, while if the outcome is β, then error occurred on first qubit, and if the outcome is γ, then error occurred on second qubit and finally, if the outcome is δ, then error occurred on the third qubit. Note that this *incomplete* measurement scheme would reveal nothing about the encoded state $|\psi\rangle$.

Recovery operation. Depending upon the outcome of syndrome measurement, the encoded state can be recovered by applying the X (Pauli σ_x) operator on the qubit identified as erroneous. The procedure works perfectly when error occurs at most on one qubit and the probability of not correcting the error is $3p^2 - 2p^3$ and is equivalent to classical repetition code. Once $p < 1/2$ the encoding and decoding improves the reliability of storing the information. Equivalently, the errors can be determined by measuring the two commuting observables Z_1Z_2 (short for $Z_1 \otimes Z_2 \otimes I$) and Z_2Z_3 (short for $I \otimes Z_2 \otimes Z_3$), where Z is Pauli σ_z. Each of the observables Z_i has eigenvalues ± 1. If Z_1Z_2 and Z_2Z_3 have measurement outcome $+1$, then no bit flip occurred. If Z_1Z_2 has measurement

outcome $+1$ and Z_2Z_3 has -1, then bit flip occurred on the third qubit. If Z_1Z_2 has measurement outcome -1 and Z_2Z_3 has $+1$, then bit flip occurred on the first qubit. If both have measurement outcomes are -1, then bit flip occurred on second qubit. The recovery operation is performed as mentioned earlier.

To improve the error analysis consider, the *fidelity* which is the measure of closeness between two given states, may be considered to quantify code performance. If ρ and σ are quantum states before and after the action of error respectively, the fidelity between them is defined as

$$F(\rho, \sigma) = \mathrm{Tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}. \tag{1.40}$$

Consider the unencoded state $|\psi\rangle$ acted upon by bit-flip noise X. The corrupt state is $(1-p)|\psi\rangle\langle\psi| + pX|\psi\rangle\langle\psi|X$. The fidelity between the corrupt and uncorrupt states is $\sqrt{(1-p) + |\langle\psi|X|\psi\rangle|^2}$. The minimum fidelity is $\sqrt{1-p}$ (say when $|\psi\rangle = |0\rangle$). Upon encoding the state as $|\psi_L\rangle = |0\rangle_L + |1\rangle_L$, the state after noise and error correction is $((1-p)^3 + 3p(1-p)^2)|\psi\rangle\langle\psi|$. The fidelity in this case is $\sqrt{(1-p)^3 + 3p(1-p)^2}$, so that encoding of qubits is beneficial if $p \leq 1/2$.

Phase flip codes

Phase-flip error is special to quantum errors and has no classical analogue. In this error model, with probability p the relative phase between the states $|0\rangle$ and $|1\rangle$ is flipped. This can be realized by applying Z (Pauli σ_z): $Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$. To construct the QECC for the error consider the states $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ which are eigenstates of X (σ_x). Notice that the action of Z takes $|+\rangle$ to $|-\rangle$ and vice versa. Thus by changing the basis from $\{|0\rangle, |1\rangle\}$ to $\{|+\rangle, |-\rangle\}$, the action of Z changes from phase flipping to bit flipping. Thus, the action of bit flip on $\{|+\rangle, |-\rangle\}$ is equivalent to phase flip on $\{|0\rangle, |1\rangle\}$. Therefore the encoding

$$|\psi_L\rangle \to \alpha|0_L\rangle + \beta|1_L\rangle \equiv \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle, \tag{1.41}$$

can protect the state $|\psi\rangle$ against phase-flip error.

For error detection, projectors $P_j' = H^{\otimes 3} P_j H^{\otimes 3}$, rotated by Hadamard gate $H = \frac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|)$, are employed. Equivalently, one uses observables X_1X_2 and X_2X_3 for error detection. If X_1X_2 and X_2X_3 have measurement outcome $+1$, then no phase-flip occurred. If X_1X_2 has measurement outcome $+1$ and X_2X_3 has -1, then phase-flip occurred on third qubit. If X_1X_2 has measurement outcome -1 and X_2X_3 has $+1$, then phase-flip occurred on first qubit. If both have measurement outcomes -1, then phase-flip occurred on second qubit. For recovery, one performs Z operation on the erroneous bit.

Illustrating quantum error correction via the Shor code

The Shor code is a QEC code that encodes one qubit in 9 qubits and provides protection against an arbitrary single-qubit error. The code is a concatenation of bit-flip and phase-flip codes. First, a state is encoded using the phase-flip code: $|0\rangle \to |++\rangle$, $|1\rangle \to |--\rangle$. Then each of these states are encoded using bit-flip codes: $|+\rangle \to \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle$, $|-\rangle \to \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$. Thus the logical states for the Shor code are

$$\begin{aligned} |0\rangle \to |0_L\rangle &\equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \\ |1\rangle \to |1_L\rangle &\equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} \end{aligned} \tag{1.42}$$

Error detection and recovery

On the first set of the three qubits, error detection is carried out similar to the 3-qubit bit-flip code. The same procedure is followed for the second and the third set of qubits. For detecting the phase-errors, consider the two observables $\mathcal{X}_1 = X_1X_2X_3X_4X_5X_6$ and $\mathcal{X}_2 = X_4X_5X_6X_7X_8X_9$. If the measurement outcomes of both $\mathcal{X}_1$ and $\mathcal{X}_2$ is $+1$, then no phase-flip occurred. If the measurement outcome of $\mathcal{X}_1$ is $+1$ and that of $\mathcal{X}_2$ is -1, then phase-flip happened on the third set of qubits. If the measurement outcome of $\mathcal{X}_1$ is -1 and that of $\mathcal{X}_2$ is $+1$, then the phase of the first set of qubits flipped. If the measurement outcomes of both $\mathcal{X}_1$ and $\mathcal{X}_2$ is -1, then phase-flip occurred on the second set of qubits. The recovery procedure is same as the 3-qubit bit flip code for each set of three qubits. For recovering the QECC from phase-flip errors, we follow the 3-qubit phase-flip code.

Discretizing quantum errors

In classical communication theory a continuum of errors is handled by *digitalizing* the signal which carry the data. In the quantum information case the errors are not only bit flip and phase flip errors but a continuum of arbitrary errors (e.g., the application of a phase gate instead of a phase flip) which might at first seem not to be correctable. But quantum error correction is possible essentially because measurement helps discretize noise. For classical analog systems, no such descretization exists.

As explained in Sec. 1.2, noise $\mathcal{E}$ on qubits has operator-sum representation with elements $\{K_i\}$ which is also the most convient for QEC. The action of noise on the QEC codes $|\psi_L\rangle$ is

$$\mathcal{E}(|\psi_L\rangle\langle\psi_L|) = \sum_i K_i|\psi_L\rangle\langle\psi_L|K_i^\dagger. \tag{1.43}$$

Discretization of continuum of the errors is achieved by decomposing K_i in the error basis

$E_j = \{I, X, Y, Z\}$ as

$$K_i = e_{i0}I + e_{i1}X + e_{i2}Y + e_{i3}Z = \sum_j e_{i,j}E_j \tag{1.44}$$

Note the the $\mathcal{E}$ could be a multi-qubit error acting on m-qubits of the QEC code. In such cases the E_i is expanded in $\{I, X, Y, Z\}^{\otimes m}$. Due to discretizition, any erroneous QEC code can be written as (apart from normalization)

$$K_i|\psi_L\rangle = e_{i0}|\psi_L\rangle + e_{i1}X|\psi_L\rangle + e_{i2}Y|\psi_L\rangle + e_{i3}Z|\psi\rangle = \sum_j e_{i,j}E_j|\psi_L\rangle, \tag{1.45}$$

due to which Eq. (1.43) can be written as

$$\mathcal{E}(|\psi_L\rangle\langle\psi_L|) = \sum_{i,j} e_{i,j}E_j|\psi_L\rangle\langle\psi_L|E_k^\dagger e_{i,k}^* = \sum_{j,k}\chi_{j,k}E_j|\psi_L\rangle\langle\psi_L|E_k^\dagger, \tag{1.46}$$

where $\chi_{i,j} = \sum_i e_{i,j}e_{i,k}^*$ is a Hermitian matrix known as the *process matrix*. The subject of quantum process tomography which deals with characterizing the quantum processes is about devising the methods to determine the process matrix $\chi_{j,k}$. This suggests that there exists overlap between QEC and quantum process tomography. This will be explored in detail in the Chapter 6 of the thesis.

By performing the syndrome measurement the state is collapsed to one of the mutually orthogonal states $|\psi_L\rangle$, $X|\psi_L\rangle$, $Y|\psi_L\rangle$, $Z|\psi_L\rangle$ which can be distinguished. For this reason, discretizing the continuum of errors works and is the central for quantum error correction. Then by performing recovery operation the QECC $|\psi_L\rangle$ is recovered.

1.3.2 Theory of quantum error correction

The theory of error correction generalizes the ideas introduced by the Shor code. In quantum information processing, a QECC protects quantum information from noise, provided the initial state $|\Psi\rangle$ is prepared within the code space $\mathcal{C}$, which satisfies suitable properties [11, 38, 35]. Let $\{|J\rangle\}$ be a n-qubit basis for $\mathcal{C}$, encoding k-qubit states $|j\rangle$ with $0 \leq j \leq 2^k - 1$. Such a code is a $((n, k))$ QECC, where k is code rate. In this work, we will assume that the error basis elements are elements of the Pauli group $\mathcal{P}_n$, the set of all possible tensor products of n Pauli operators, with and without factors $\pm 1, \pm i$. Thus $E_k^\dagger = E_k$ and $(E_j)^2 = I_n$, the identity operator over n qubits. The necessary and

sufficient conditions for quantum error correction are:

$$\langle J|E_m^\dagger E_n|K\rangle = 0 \tag{1.47a}$$

$$\langle J|E_m^\dagger E_n|J\rangle = \langle K|E_m^\dagger E_n|K\rangle \in \{0,1\} \tag{1.47b}$$

where $|J\rangle \neq |K\rangle$, and E_m, E_n are two (possibly identical) basis elements of an operator basis for the space $\mathcal{E}$ of allowed errors. In Eq. (1.47b), the choice 0 corresponds to the non-degenerate case.

To see why Eqs. (1.47) are necessary, suppose that the total recovery operation is denoted by a unitary operation $\mathcal{R}$. Recovery involves preparing an ancilla in an initial state $|\alpha\rangle$ and applying $\mathcal{R}$ on the joint system. We thus have $\mathcal{R}|\alpha\rangle E_m|J\rangle = |\alpha_m\rangle|J\rangle$ and $\mathcal{R}|\alpha\rangle E_n|K\rangle = |\alpha_n\rangle|K\rangle$, or

$$\begin{aligned} \langle J|E_m\langle\alpha|\mathcal{R}^\dagger\mathcal{R}|\alpha\rangle E_n|K\rangle &= \langle\alpha_m|\alpha_n\rangle\langle J|K\rangle \\ \Rightarrow \langle J|E_m E_n|K\rangle &= 0, \end{aligned}$$

from which Eq. (1.47a) follows. This ensures that two distinct code words are not confused even in the presence of noise, and has an obvious counterpart in classical error correction. We also have

$$\begin{aligned} \langle J|E_m\langle\alpha|\mathcal{R}^\dagger\mathcal{R}|\alpha\rangle E_n|J\rangle &= \langle\alpha_m|\alpha_n\rangle \\ \Rightarrow \langle J|E_m E_n|J\rangle &= \langle\alpha_m|\alpha_n\rangle, \end{aligned}$$

as also for $|K\rangle$, from which Eq. (1.47b) follows. Note that we only require for equality between the left- and right-hand sides of Eq. (1.47b). If in addition the lhs and rhs vanish, this would correspond to the classical requirement that distinct errors on the same code word produce orthogonal erroneous words. In the quantum case, however, the lhs and rhs need not vanish, and we obtain *degenerate* codes, which have no classical counterpart.

To prove the sufficiency of (1.47) for quantum error correction, let the system be in an arbitrary logical state $|\Psi\rangle = \sum_J \alpha_j|J\rangle$, which encodes the state $|\psi\rangle = \sum_j \alpha_j|j\rangle$, where $\sum_j |\alpha_j|^2 = 1$. Let the error be an incoherent sum of Kraus operators of the form $F = \sum_k \beta_k E_k$, with $\sum_k \beta_k = 1$. This maps the initial state to $F|\Psi\rangle$. In the non-degenerate case, $F|\Psi\rangle = \beta_0 E_0|\Psi\rangle + \cdots \beta_{4^n-1}E_{4^n-1}|\Psi\rangle$. Each of the terms $E_j|\Psi\rangle$ must be in an orthogonal space given (1.47). Thus, a projection to $E_j\mathcal{C}$, followed by an application of E_j constitutes the required recovery $\mathcal{R}$. In the degenerate case, suppose that E_m and E_n are degenerate. Then $E_m|J\rangle = E_n|J\rangle$, and a projection on to $E_m\mathcal{C} = E_n\mathcal{C}$ followed by either E_m or E_n constitutes the required recovery $\mathcal{R}$.

The conditions (1.47) can be equivalently stated [35]:

$$\langle \Psi | G^\dagger G | \Psi \rangle = c(G), \tag{1.48}$$

where the function c depends only on the error G and not the encoded state $|\Psi\rangle$. By expanding $|\Psi\rangle$ in terms of $|J\rangle$ and G in terms of the basis elements E_j, we rewrite condition (1.48) as:

$$\langle J | E_m^\dagger E_n | K \rangle = c_{m,n} \delta_{JK}, \tag{1.49}$$

where $c_{m,n}$ is a Hermitian matrix of numbers that is independent of J, K.

Bounds on quantum error correcting codes

The quantum versions Hamming and Gilbert-Varshamov bounds were introduced by Ekert and Macchiavello [36]. Consider a k-qubit state being encoded into a n-qubit QEC code and at most independent single qubit errors happen on t-qubits. The possible errors are X, Y, Z. Also there are 2^k such logical states. The total number of possible errors is $\sum_{j=0}^{t} {}^nC_j 3^j$. For non-degenerate codes the total number of errors must be lesser or equal to 2^n. Thus we have the inequality

$$2^k \sum_{j=0}^{t} {}^nC_j 3^j \leq 2^n \tag{1.50}$$

For $k = 1$ and $t = 1$ the quantum Hamming bound reduces to $2(1 + 3n) \leq 2^n$. The inequality is not satisfied for $n \leq 4$, while for $n \geq 5$ it is. There for there is no code with less than five qubits which can protect a qubit against the single qubit errors. However, in the Chapter 7 we introduce a class of codes called as ambiguous stabilizer codes, that generalizes the degenerate codes and can violate the Bound.

For large n and some k there exists $[n, k]$ code correcting errors on at most t-qubits such that

$$\frac{k}{n} \geq 1 - 2H\left(\frac{2t}{n}\right), \tag{1.51}$$

where $H(x)$ is the binary Shannon entropy and the bound is known as Gilbert-Varshamov bound.

1.3.3 Stabilizer codes

A stabilizer description of error correction [39, 51] is advantageous in focussing attention on operators, which can be compact, rather than on code words, which can be large. A state $|\psi_L\rangle$ is said to be stabilized by an operator S if $S|\psi_L\rangle = |\psi_L\rangle$. Let $\mathcal{G}$ be a subset of

$n-k$ independent, commuting elements from $\mathcal{P}_n$. A $[[n,k]]$ QECC is the 2^k-dimensional $+1$-eigenspace $\mathcal{C}$ of the elements of $\mathcal{G}$. The simultaneous eigenbasis of the elements of $\mathcal{G}$ are the code words $|j_L\rangle$. The set of 2^{n-k} operators generated by $\mathcal{G}$ constitute the stabilizer $\mathcal{S}$. The centralizer of $\mathcal{S}$ is the set of all elements of $\mathcal{P}_n$ that commute with each member of $\mathcal{S}$:

$$\mathcal{Z} = \{P \in \mathcal{P}_n \mid \forall S \in \mathcal{S}, [P,S] = 0\}, \tag{1.52}$$

while the normalizer of $\mathcal{S}$ is the set of all elements of $\mathcal{P}_n$ that conjugate the stabilizer to itself:

$$\mathcal{N} = \{P \in \mathcal{P}_n \mid P\mathcal{S}P^\dagger = \mathcal{S}\}. \tag{1.53}$$

We note that $\mathcal{S} \subseteq \mathcal{N}$ because the elements of $\mathcal{S}$ are unitary and mutually commute. Similarly, $\mathcal{Z} \subseteq \mathcal{N}$ because elements of the centralizer are unitary and commute with all elements of the stabilizer. To see that the converse is true, we note that if $N \in \mathcal{N}$ then $NSN^\dagger = S'$, or $NS = S'N$. For Pauli operators, $NS = \pm SN$, meaning $S' = \pm S$. But if $S' = -S$, then $NSN^\dagger = -S$, which would require that both S and $-S$ are in $\mathcal{S}$. However if $S \in \mathcal{S}$, then $-S$ is not in the stabilizer, so the only possibility is $S' = S$, and we obtain $[N,S] = 0$, i.e., $\mathcal{N} \subseteq \mathcal{Z}$. It thus follows that here $\mathcal{Z} = \mathcal{N}$. We have $SN|j_L\rangle = NS|j_L\rangle = N|j_L\rangle$, which implies that the action of N is that of a logical Pauli operation on code words.

A set of operators $E_j \in \mathcal{P}_n$ constitutes a basis for correctable errors if one of the following conditions hold:

$$E_j E_k \in \mathcal{S} \tag{1.54a}$$

$$\exists G \in \mathcal{G} : [E_j E_k, G] \neq 0. \tag{1.54b}$$

The case (1.54a) corresponds to *degeneracy*. Here $\langle\psi_L|E_jE_k|\psi_L\rangle = \langle\psi_L|\psi_L\rangle = 1$, meaning that both errors produce the same effect, and the code space is indifferent as to which of them happened. Thus either error can be applied as a recovery operation when one of them occurs. The case (1.54b) corresponds to $E_j^\dagger E_k \notin \mathcal{N}$. In that case, $\exists G \in \mathcal{G} : E_jE_kG = -GE_jE_k$, which ensures that G anti-commutes with precisely one of the operators E_j and E_k. Thus the noisy logical states $E_j|\psi_L\rangle$ and $E_k|\psi_L\rangle$ will yield distinct eigenvalues (one being $+1$ and the other -1) when G is measured. The set of $n-k$ eigenvalues of ± 1 obtained by measuring the generators G forms the error syndrome. The consolidated error correcting condition (1.54) can be stated as the requirement $E_jE_k^\dagger \notin \mathcal{N} - \mathcal{S}$.

1.4 Noise characterization

Characterizing the quantum dynamics forms a vital part in implementing quantum computation and information physically. This provides a comparison of the implemented quantum operations against the desired ones on the qubits and thus helps in benchmarking the quality of gates. Also, principal difficulty in realizing the quantum processing tasks is due to environmental-induced noise (unnecessary dynamics), which decoheres the quantum system, resulting in the loss of quantum superposition and entanglement. In this situation, complete or partial characterization of noise is essential to fight against it, say by constructing appropriate quantum error correcting codes.

Action of noise $\mathcal{E}$, described by a CP map, on a quantum state ρ of dimension d can be expressed in an error basis $\{E_i\}$ for $d \times d$ matrices as described by Eq. (1.46) in Sec. 1.3

$$\mathcal{E}(\rho) = \sum_{m,n}^{d^2} \chi_{m,n} E_m \rho E_n^\dagger. \tag{1.55}$$

The error basis $\{E_i\}$ satisfies the orthogonality condition $\mathrm{Tr}(E_i E_j^\dagger) = d\delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta. $\chi_{m,n}$ is a Hermitian matrix, also known as the "process matrix", in the d^2-dimensional Hilbert-Schmidt space of linear operators acting on the system of dimension d. From the tracing preserving property of $\mathcal{E}$, we have $\sum_{m,n}^{d^2} \chi_{m,n} E_m^\dagger E_n = \mathbb{I}$, which imposes d^2 conditions, so that the matrix χ has $d^4 - d^2$ independent real elements. This forces the condition $\sum_j \chi_{j,j} = 1$, the (positive) diagonal elements of which can be interpreted as probabilities. In this work, E_j are multi-qubit Pauli operators, which is appropriate for employing the QEC formalism.

1.4.1 Standard quantum process tomography

Characterization of a quantum noise is determining the elements of process matrix $\chi_{m,n}$. The first technique to address this was standard quantum process tomography (SQPT) [11, 52] where a set of suitably prepared states $\{\rho_i\}$ is input to unknown noisy dynamics $\mathcal{E}$ to be characterized. The action of $\mathcal{E}$ on each input state can be determined experimentally by the state tomographic techniques as

$$\mathcal{E}(\rho_i) = \sum_k C_{i,k} \rho_k, \tag{1.56}$$

where $\{\rho_k\}$ is a basis for measurements on output states of $\mathcal{E}$ and $C_{i,k} = \mathrm{Tr}(\mathcal{E}(\rho_i)\rho_k)$ are measurement out comes. Also $E_m \rho_i E_n^\dagger = \sum_k \beta_{i,k}^{m,n} \rho_k$, where $\beta_{i,k}^{m,n}$ is matrix determined by the choice of $\{\rho_i\}$, $\{\rho_k\}$ and $\{E_i\}$. substituting the expression in Eq. (1.55) and

comparing with Eq. (1.56) we have

$$\sum_k \sum_{m,n} \chi_{m,n} \beta_{i,k}^{m,n} \rho_k = \sum_k C_{i,k} \rho_k. \tag{1.57}$$

Obtaining the values of $C_{i,k}$ from state tomographic measurements one can determine the elements of the process matrix to be $\chi_{m,n} = \sum_{i,k} (\beta_{i,k}^{m,n})^{-1} C_{i,k}$. By SQPT, one needs to perform $d^4 - 1$ measurements which grows exponentially with number of qubits.

1.4.2 Ancilla-assisted process tomography

Another method to determine the $\chi_{m,n}$ is ancilla-assisted process tomography (AAPT) where the principal system **P** and an ancillary system **A** are prepared in suitable initial states. Noise to be characterized $\mathcal{E}$ is made to act on **P** while **A** is required to be clean. The initial state considered in Ref. [53] was an entangled state, not essentially maximally entangled, and later it was showed in Ref. [54] that even a non-entangled Werner state can be used. The information about the dynamics on **P** is extracted via quantum state tomography on the joint system using separable or non-separable basis measurements. By having the ancilla of dimension atleast equal to that of principal system it is guaranteed that the joint state after subjected to noise will bear one to one correspondence with the noise [54]. $d^4 - 1$ measurements are needed using separable measurements where as the same can be achieved by d^2 with non-separable measurements [55].

1.4.3 Direct methods

SQPT and AAPT are not direct methods for QPT in the sense that they first obtain full state tomographic data of the out put states of the channel $\mathcal{E}$, and then use this exponentially large (grows with number of qubits) data to derive χ. Subsequently, a method which bypasses the state tomography known as direct characterization of quantum dynamics (DCQD) was introduced in Ref. [56, 57]. DCQD uses the maximally entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$ stabilized by ZZ and XX for determining the diagonal terms of χ. The detection of error i.e., syndrome measurement is implemented via Bell state measurements. For determining the off-diagonal terms, stabilizer measurement non-maximally entangled states $\alpha|00\rangle + \beta|11\rangle$ (stabilized by ZZ), where $\alpha \neq \beta$, is performed. The statistics of measurement out comes can determine an offdiagonal term. Then on the stabilizer-measurement-collapsed states normalizer (XX) measurement (which commutes with stabilizer) is done to get other offdiagonal term. The complete process matrix can be determined by using d^2 different input states and single measurement on each state. Totally, $d^2 - 1$ configurations are needed. Other recent developments include a character-

ization of noise using an efficient method for transforming a channel into a symmetrized (i.e., having only diagonal elements in the process matrix) channel via twirling [58], which is suitable for identifying QECCs [59]. A method similar to [58], but extended to estimate any given off-diagonal term, was introduced in Ref. [60].