1
Preliminaries and literature survey

1.1 INTRODUCTION

During the last three decades, the field of quantum technology has received a lot of public attention, all due to the efforts from academia and industry to bring quantum information and computation at the verge of technology development. The fusion of fundamental laws of quantum mechanics with computing and information theory has led the path towards performing computation in the quantum realm. The significant development towards shifting the computing paradigm from classical to quantum- and from theory to technological implementation- can be attributed to groups of researchers across the globe and multinational companies like IBM, Google, D-wave, Microsoft, Honeywell, Ion Q, Intel, Hewlett Packard, Regetti, Cambridge quantum computing and Quantum Biosystems, to name a few. Recent developments show that several startups have also been established in the emerging field of quantum information and computation. All the research and development in this field is indeed inspired from the inherent characteristics of quantum physics such as *superposition principle*, *interference* and *quantum entanglement*. Using these quantum phenomena, classically hard problems can be solved relatively quickly. For example, the existing cryptography protocols, relying on the hardness of some mathematical problems like prime factorization and discrete logarithms, face real threats from quantum algorithms. With the advent in quantum technologies, quantum algorithms- Shor's algorithm [Shor, 1999]- can solve these classically hard prime factorization and discrete logarithm problems in polynomial time which are highly difficult or even impossible using classical resources. A fault-tolerant scalable quantum computer, therefore, can definitely be used to break several cryptographic protocols. However, due to quantum noise and limiting size of quantum circuits, i.e., in the noisy intermediate-scale quantum (NISQ) era [Preskill, 2018], it is practically impossible to break current cryptography protocols in the present time. Yet, quantum algorithms give exciting speedup for particular problems like searching, optimization and other algebraic problems [Grover, 1997; Hogg and Portnov, 2000; Childs and Van Dam, 2010; Sun *et al.*, 2012a; Childs *et al.*, 2018; Tang, 2021]. Considering the advancement in quantum technologies, the National Institute of Standards and Technology (NIST) in 2017 initiated a post-quantum cryptography standardization process intended to standardize cryptographic protocols capable of protecting sensitive information from future quantum computers [Moody *et al.*, 2020]. Quantum technologies can also change the way chemistry simulations are done [Lanyon *et al.*, 2010; Hastings *et al.*, 2015; Cao *et al.*, 2019; Yuan *et al.*, 2021]. The instances such as using quantum algorithms for fermionic simulations [Ortiz *et al.*, 2001], calculating the thermal rate constant with exponential speedup on a quantum computer [Lidar and Wang, 1999] and simulating molecular energies [Aspuru-Guzik *et al.*, 2005; Wang *et al.*, 2008; O'Malley *et al.*, 2016] can further be extended to the fields of agriculture [Villaverde *et al.*, 2017], material science [Bauer *et al.*, 2020], and pharmaceutical applications [Cassens *et al.*, 2010; Lam *et al.*, 2020]. Atallah and Atallah showed the potential of quantum technologies for the next-generation digital surgeries [Atallah and Atallah, 2021]. The fact that quantum computers can solve some particular problems faster than the fastest classical computer, finance industry is also going to be affected [Schaden, 2002; Orus *et al.*, 2019; Egger *et al.*, 2020; Ziemann, 2021] through reducing the complexity of finance [Baaquie *et al.*, 2003], by providing speed-up using Monte Carlo simulations for pricing of financial derivatives [Rebentrost *et al.*, 2018], and through portfolio optimization [Kerenidis *et al.*, 2019].

One of the most fundamental differences between classical and quantum approach to computing is laid down in terms of quantum parallelism. The basic units of quantum computation are qubits which can be represented as an arbitrary linear superposition of orthonormal eigenstates of the property being measured. For an n qubit state, there are 2^n basis states which can be encoded and processes at once due to the superposition and linearity being the characteristic features of quantum mechanics- this leads to the concept of quantum parallelism which cannot be simulated by fastest of classical computers in polynomial time. On the implementation front, one needs to address issues of controlling, manipulating, scaling and accessing of quantum information. Nevertheless, there are tireless efforts to address these and many other technological challenges to put efficient developments on the pedestal of a fault-tolerant quantum computer. Clearly, entanglement and nonlocality are at the cornerstone of the basic premise of quantum information and computation. Initially, entanglement was believed to be the only key resource responsible for efficient applications in quantum information processing [Bennett and Brassard, 1984; Bennett and Wiesner, 1992; Bennett *et al.*, 1993; Steane, 1998; Karlsson and Bourennane, 1998; Hillery *et al.*, 1999]. While the importance of entanglement is incontestable, other features of quantum theory have also been proved to play a crucial role towards the much discussed quantum advantages. One of these features is nonlocality- since quantum mechanics itself is nonlocal, the nonlocality refers to the stronger-than-classical connections between the distant objects; and although it may be further considered as an obvious expression of entanglement, the two are not equivalent. Moreover, it is now well established that nonlocality and entanglement are two different concepts [Brunner *et al.*, 2005]. With the advancements in the field, nonlocality has also been recognized as a resource [Ekert, 1991; Schuch *et al.*, 2004; Barrett *et al.*, 2005; Acin *et al.*, 2006; De Vicente, 2014; Curchod *et al.*, 2014; Camalet, 2020; Niezgoda and Chwedeńczuk, 2021] for quantum information theory. The discussions on nonlocal correlations can be traced back to Einstein-Podolsky-Rosen paradox [Einstein *et al.*, 1935] and design of the Bell inequality based on the assumptions of locality and realism [Bell, 1964]. In 1964, John S. Bell with his seminal proposal established a clear boundary between locally explainable correlations between two particles versus correlations which can not be explained by local realistic theories and are thus nonlocal. Following the Bell inequality, multiple variations of the same were further introduced to study nonlocal behavior of quantum systems- generally known as Bell-type inequalities [Pascazio, 1986; Svetlichny, 1987; Collins *et al.*, 2002; Seevinck and Svetlichny, 2002; Gisin *et al.*, 2007; Shchukin and Vogel, 2008; Loubenets, 2008; Deng *et al.*, 2009; Akopyan *et al.*, 2010; Pál and Vértesi, 2011; Bancal *et al.*, 2011, 2012; Curchod *et al.*, 2014; Sun *et al.*, 2014; Home *et al.*, 2015; He *et al.*, 2015; Liang *et al.*, 2015; Sun *et al.*, 2015; Tavakoli, 2016; Taddei *et al.*, 2016; Barasiński and Nowotarski, 2018; Sun *et al.*, 2019; Xue and Qiu, 2020; Sun *et al.*, 2021]. The violation of these Bell and Bell-type inequalities by quantum systems have been considered to characterize genuine nonlocality in bi-partite and multiqubit systems. However, there exists instances where the Bell inequality in bi-partite mixed entangled systems or Bell-type inequalities in multiqubit entangled pure systems fail to identify nonlocal correlations in underlying states. Discord, for that matter, measures non-classical correlations in all bi-partite pure and mixed entangled and separable states. Moreover, several multiqubit Bell-type inequalities further suffer from indistinguishability between genuine multiqubit nonlocality and nonlocality resulting due to entanglement of product states within subsystems. Although we have witnessed several significant studies towards characterization and generalization of entanglement and nonlocality in multiqubit systems, there is no generic mechanism to characterize or generalize the study to analyze genuine nonlocal correlations from bi-partite systems to multiqubit systems. Therefore, we require a more generic and comprehensive approach for identifying, analyzing and characterizing nonlocal correlations in bi-partite and multiqubit entangled systems.

In the present doctoral research work, efforts are made to develop efficient operators that can identify genuine nonlocal correlations in maximally as well as partially entangled bi-partite and multiqubit states in a systematic manner. In addition, we further study efficiencies of partially entangled multiqubit states as resources for quantum information processing protocols in real

conditions.

This chapter begins with a brief introduction to basic terminologies and concepts in quantum information and computation including a description of noise and information processing protocols. We further discuss the background, motivation and relevance to the research problems addressed in this Thesis. We finally discuss our research objectives followed by the main contributions towards the Thesis. The chapter concludes with a chapter-wise outline of the Thesis.

1.2 BASICS OF QUANTUM INFORMATION AND COMPUTATION

The paradigm shift in computing from classical to quantum is due to the inherent nature of quantum systems, i.e., to be able to exist in a superposition state of eigenvectors of an operator. This very fundamental property of the theory allows the fundamental unit of quantum information and computation- a qubit- to be represented as an arbitrary linear superposition of the two orthonormal basis vectors $|0\rangle$ and $|1\rangle$. In fact a qubit can be represented in infinitely many ways by using a basis which satisfies the conditions to be an orthonormal basis set. Initially it was considered that this linear superposition in certain cases allows quantum resources to administer speed and space advantage in comparison to its classical counterparts. In the last three decades, together the academic community and the industry has witnessed countless instances of efficient applications of quantum resources which are impossible to achieve using classical resources. Although a qubit can be represented using the linear superposition of all possible basis vectors, a measurement to identify the state of a qubit results in collapse of the original quantum state to one of the eigenvectors of the operator being measured. For example, if one measures the state of a qubit with the field in Z-direction, then the system is either forced to be in $|0\rangle$ or in $|1\rangle$ state with respective probabilities such that the sum of probabilities leads to 1. Nevertheless, the applications of quantum information and computation are being recognized by diverse academic domains including communication, security, finance, defense, deep learning and machine learning, optimization, image processing, computational chemistry and biology, to name a few. At the heart of all these applications are entanglement, nonlocality and quantum correlations. The inception of these concepts can be traced back to 1935 when Einstein, Podolsky and Rosen (EPR) started an intellectual debate by raising questions on whether quantum theory can be considered as a complete physical theory or not. Since then, the academic community across the globe has excitedly witnessed the analysis on investigations and applications of foundations of quantum theory.

For two or more than two qubits, the linear superposition of basis states can lead to a decisive phenomenon termed as entanglement by Erwin Schrodinger. The entangled systems are defined using a joint state of all qubits such that the state of subsystems cannot be defined independently. Clearly, the properties of each of the subsystems depend on the properties of other subsystems forming the entangled state. The long-range nonlocal correlations existing between entangled qubits with no classical analogue further allow such systems to violate the fundamental Bell or Bell-type inequalities thereby differentiating the quantum world from its classical counterpart. The violation of Bell inequality- designed based on the assumptions of locality and realism- by entangled systems sheds light on the distinct nature of nonlocal correlations as against the classical correlations. Therefore, quantum nonlocality refers to the phenomenon by which the measurement statistics of a multiqubit system do not admit an interpretation in terms of local realistic theories. One of the most celebrated two-qubit entangled states exhibiting nonlocal correlations are the four Bell or EPR states. These states are considered to be the maximally entangled two qubit states violating the Bell inequality maximally, and have extensively used in literature for numerous potentially efficient applications in quantum information and computation. Initially entanglement and nonlocality have been used interchangeably, but now it has been clearly established that these are two distinct measures. The

concept of nonlocality or quantumness goes beyond the boundaries of quantum entanglement and can be extended to separable systems as well. For example, quantum discord demonstrates the existence of nonlocal correlations in entangled as well as separable systems, therefore, discord is considered as a genuine measure of quantumness in an underlying quantum state.

In the following subsections, we briefly describe some of the basic terminologies and key concepts of quantum information and computation.

1.2.1 Qubit: the fundamental unit of quantum information and computation

In classical computation, the information is encoded in form of strings of bits where the state of a *bit* can be represented by binary digits 0 or 1. The information can then be manipulated using logic gates to map one form of the information to another. For example, some of the standard logic gates are AND, OR, NAND, NOR and NOT gates. The NOT gate is distinctly different from all other logic gates in terms of the equality of number of inputs and outputs before and after the application of gates, respectively. In general for all logic gates, except the NOT gate, one needs to use two inputs to obtain one output. The inputs are therefore represented by the initial states of bits and output is represented by the final state of bits after the operation of logic gates. Clearly, in case of logic gates, one would not be able to decipher the input states given a certain output, e.g., using an AND gate if the output is 0, one would not be able to say whether the input was 00, 01, or 10. Therefore, the logic gates are considered to be irreversible in nature as we cannot always reconstruct input states given a particular output. In fact, Landauer [Landauer, 1961] has shown that this deletion of information- due to the irreversible nature of logic gates- results in dissipation of energy as a classical computer performs computation. This should not be surprising as deleting information requires work which leads in dissipation of energy in form of heat. In addition to the logical reversibility, one further needs to consider thermodynamical reversibility for the computation to ensure no dissipation of energy as a heat loss [Fredkin and Toffoli, 1982; Bennett, 1988]. The problem can be addresses using gates which are reversible in nature along with thermodynamical reversibility. Interestingly, quantum gates being unitary in nature are reversible and the same will be discussed in a later section.

Analogues to bits, quantum computation relies on a similar fundamental resource called as quantum bits or Q-bits or *qubits*. The state of a qubit can be represented using two orthonormal basis states $|u_1\rangle$ and $|u_2\rangle$ such that $|\psi\rangle = a|u_1\rangle + b|u_2\rangle$. Clearly, there is a distinct difference between the two fundamental units of computations, i.e. between bits and qubits such that the state of a qubit can not only be represented by $|u_1\rangle$ or $|u_2\rangle$ but also by an arbitrary linear superposition of $|u_1\rangle$ and $|u_2\rangle$. The fundamental laws of quantum mechanics therefore allow one to represent the state of a qubit using both the basis states at once. This is a remarkable phenomenon with no classical analogue, and results in quantum parallelism once we move from a single qubit to multiple qubit states. As a standard notation qubits are represented using *Dirac* or *Bra-Ket* notations where the notations $|\rangle$ and $\langle|$ are known as *ket* and *bra*, respectively. Hence, in terms of the Dirac's notations, the state of a qubit is described as $|\psi\rangle$ which therefore is pronounced as 'ket-ψ'. As a standard notation, we represent the state of a qubit using the computational basis $|0\rangle$ and $|1\rangle$ as

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

where α and β are complex coefficients representing probability amplitudes associated with $|0\rangle$ and $|1\rangle$ states, respectively. Precisely, if one performs a measurement in computational basis to reveal the state of a qubit, then the possible outcomes are $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$. Since the total probability must add up to 1, coefficients α and β must satisfy the following condition which is also known as the normalization condition, i.e.,

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.2}$$

Geometrically, the state of a qubit can be defined as a vector in a two-dimensional complex vector space where $|0\rangle$ and $|1\rangle$ represent vectors in the two-dimensional Hilbert space. Algebraically, using the standard notation, $|0\rangle$ and $|1\rangle$ states can be further defined as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.3}$$

Considering that the inner product of two vectors $|x\rangle$ and $|y\rangle$ is defined as $\langle x|y\rangle$, $|0\rangle$ and $|1\rangle$ clearly form an orthonormal basis set such that

$$\langle 0|1\rangle = \langle 1|0\rangle = 0$$
$$\langle 0|0\rangle = \langle 1|1\rangle = 1$$

One can therefore re-express the state of a qubit represented in Eq. (1.1) using Eq. (1.3) as

$$|\psi\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{1.4}$$

1.2.2 Density operators- pure versus mixed states

In classical mechanics, the very knowledge of initial conditions and the forces acting on the system of interest allows one to predict the future motion of the system using the dynamical equation of motion. However, for quantum mechanical systems, one does not have access to such a maximal set of information due to the fundamental Heisenberg uncertainty principle [Heisenberg, 1977; Busch *et al.*, 2007]. Therefore, the dynamics of a quantum system needed to be described by introducing a new physical theory, i.e., either by using Schrodinger's wave mechanics or Heisenberg's matrix mechanics. The solutions of the Schrodinger equation is interpreted using wave functions which provide a complete mathematical description of the system under study. The wave functions can be described as eigen functions of commuting operators or corresponding observables. However, if one measures a property such that the system under study is not in eigenstates of the corresponding operator then the statistical character of measurement process comes into the picture. Moreover, preparing different components of a composite system independently further leads to an additional statistical character to measurement process such that only the subsystems can be represented by state vectors with certain probabilities, and not the composite state. In general, the ensemble of spins- irrespective of whether one has maximal information or less than the maximal information about the preparation of system- can be most suitably described by a statistical operator known as the density operator [Fano, 1957; Chuang and Nielsen, 2010; Blum, 2012]. The density operator or density matrix is therefore an alternate mathematical representation of the state of a quantum system, generally denoted by the symbol ρ. If the state can be characterized by a single wave function then the density matrix is formally defined as the outer product of quantum state and its conjugate transpose, i.e., the density matrix ρ for the state $|\psi\rangle$ is given by

$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} \tag{1.5}$$

where $'*'$ represents complex conjugation. In general the state of a quantum system may or may not be defined using a single wave function. A statistical mixture can be defined as a convex combination of ensemble of pure states such that

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{1.6}$$

where p_i represents the probability associated with the measurement outcome $|\psi_i\rangle$. The state represented in Eq. (1.5) is a pure state, whereas the statistical mixture represented in Eq. (1.6) is

a mixed state. In case of mixed states, different parts of the system will be oriented in different directions with certain probabilities such that the joint state can never be represented using a single state vector. Experimentally, if one sends a beam of pure state through a Stern-Gerlach (SG) device with inhomogeneous magnetic field then it is always possible to determine an orientation of the SG device so that the complete beam is transmitted through the device. On the other hand, in case of mixed states, no such orientation can be found as one cannot define a single state vector for the statistical mixture and hence only part of the beam can be transmitted through the SG device, corresponding to a particular measurement outcome. One can follow the definition of pure and mixed states by realizing that mixed states are result of a joint state where different components are prepared independently to one other resulting in no distinct phase relation between components which clearly is not the case with pure states. For example $|\psi_1\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$ and $\rho_1 = \frac{1}{2}[|0\rangle\langle 0| + |1\rangle\langle 1|]$ are two distinct representations of a single qubit state; $|\psi_1\rangle$ represents a pure state oriented in the $+X$ direction therefore if the magnetic field in SG device is also oriented in the $+X$ direction, all such particles will pass through the device unattenuated. Whereas ρ_1 represents a mixed state such that one half of the system is oriented in $+Z$ direction or other half of the system is oriented in $-Z$ direction leading to the attenuation of the transmitted beam when sent through the SG device. Therefore, density operator formalism is a very convenient mathematical tool to describe a statistical mixture or in general any quantum state. A density operator formalism contains all the relevant information about the preparation of the system and satisfies the following properties

1. Unit trace: $Tr(\rho) = 1$
2. Hermitian: $\rho = \rho^\dagger$
3. Positive: $\langle u|\rho|u\rangle \geq 0$ for all vectors $|u\rangle$

The diagonal elements of a density operator represent probabilities of finding the system in respective basis states, therefore the trace of a density operator is a sum of all such probabilities which naturally leads to unity. Moreover, one can also evaluate $Tr(\rho)$ of a density operator defined in Eq. (1.6) to be unity where Tr represents the trace operation such that $Tr(\rho) = \sum_i p_i Tr(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1$. The last two conditions enumerated above signify a density operator (ρ) must have real and non-negative eigenvalues.

A single qubit density operator can be defined using a linear superposition of a $2\otimes 2$ identity operator I and three Pauli operators σ_x, σ_y, and σ_z, i.e.,

$$\rho = \frac{1}{2}[I + P_i.\sigma_i] \tag{1.7}$$

where P represents the polarization vector, associated with the state of qubit, whose three components can be defined as $P_i = \langle\sigma_i\rangle$. Clearly, a pure state can be characterized by a polarization vector of unit magnitude oriented in a specific direction, and a mixed state can be characterized by a polarization vector of less than unit magnitude. Using Eq. (1.7), algebraically one can further characterize a density operator to be either pure or mixed by evaluating $Tr(\rho^2) \leq 1$- an equality confirms the state to be a pure state else it is a mixed state. Another important criterion to distinguish between pure and mixed states is entropy, i.e., $S(\rho) = -Tr(\rho log[\rho])$ or $S(\rho) = -\sum_k \lambda_k log\lambda_k$ where λ_k are eigenvalues of ρ [Von Neumann, 1927; Van Hove, 1958]. Considering pure states to be states with maximal information there is no degree of uncertainty associated with pure states thus the entropy is 0. On the other hand, mixed states are states with less than the maximal information, therefore, there is a degree of uncertainty associated with such states and hence the entropy $S(\rho) > 0$.

The density operator formalism allows one to capture several important characteristics of an ensemble of qubits and has been extensively used to study and analyze nuances of quantum

information and computation [Ter Haar, 1961; Aslangul and Kottis, 1978; White, 1992; Hughston *et al.*, 1993; Hall, 1998; Osborne and Nielsen, 2002; Das *et al.*, 2003; Cattarius and Meyer, 2004; Verstraete *et al.*, 2004b; Viamontes *et al.*, 2004; Micha, 2006; Hallberg, 2006; Ohtsuki and Fujimura, 2007; Legeza *et al.*, 2008; Koller *et al.*, 2010; Pop *et al.*, 2013; O'brien *et al.*, 2017; Šafránek, 2018; Xu *et al.*, 2020a; Reimer and Wegewijs, 2019; Aremua *et al.*, 2021a,b]. Moreover, the use of wave function/spin state picture to describe multiqubit states or information processing protocols under real scenario does not provide a convenient description of experimental observations of decoherence in quantum systems. Building a theory based on the density matrix approach enables the theorist to parameterize decoherence in terms of statistical correlations (coherences) which are described adequately by off-diagonal matrix elements of the density operator in an appropriately chosen basis. Probably, one of the most celebrated applications of the density operator is characterizing the properties of subsystems of a composite quantum mechanical state. Such a descriptive tool- known as a *reduced density operator*- further lays down the foundations to understand the intricacies involved in analyzing the mechanisms of a decoherence process. Specifically, if ρ_{12} is the density operator of a composite system of two qubits, then the reduced density operator associated with qubit 1 (or qubit 2) can be represented as $\rho_1 = Tr_2(\rho_{12})$ (or $\rho_2 = Tr_1(\rho_{12})$). For example, if the composite state of two qubits is defined as $\rho_{12} = |\psi_{12}^-\rangle\langle\psi_{12}^-|$ where $|\psi_{12}^-\rangle = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]$, then the reduced density operators associated with individual subsystems can be represented as $\rho_1 = \rho_2 = \frac{I}{2}$. The concept of reduced density operator is highly effective and convenient to study several concepts in quantum information and computation [Donnelly and Parr, 1978; Jacyna-Onyszkiewicz, 2002a,b; Peschel, 2004; Cances *et al.*, 2006; Rice, 2007; Sharma *et al.*, 2008; Casini and Huerta, 2009; Micha and Leathers, 2009; Fagotti and Essler, 2013; Jacobs, 2014; Mostafanejad and DePrince III, 2018; Jacyna-Onyszkiewicz, 2018; Cioslowski, 2020; Chen *et al.*, 2021].

1.2.3 The Bloch sphere

As discussed in one of the previous subsections, the general state of a single qubit can be represented as an arbitrary linear superposition of two orthonormal basis states, e.g., $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where the state of the qubit is expressed in terms of eigen vectors of the σ_z operator. Considering that α and β are coefficients in a complex vector space, we can assume $\alpha = e^{\iota\phi_1}Cos(\gamma)$ and $\beta = e^{\iota\phi_2}Sin(\gamma)$ such that the general state of a single qubit can be equivalently represented as

$$\begin{aligned}|\psi\rangle &= e^{\iota\phi_1}Cos(\gamma)|0\rangle + e^{\iota\phi_2}Sin(\gamma)|1\rangle \\ &= e^{\iota\phi_1}\left[Cos(\gamma)|0\rangle + e^{\iota(\phi_2-\phi_1)}Sin(\gamma)|1\rangle\right]\end{aligned} \tag{1.8}$$

where $\iota = \sqrt{-1}$ and γ and ϕ_i are real parameters. In Eq. (1.8), $e^{\iota\phi_1}$ is a global phase factor which has no physical interpretation or observable effect in quantum mechanics, therefore, Eq. (1.8) can be re-expressed as

$$|\psi\rangle = Cos(\gamma)|0\rangle + e^{\iota\phi}Sin(\gamma)|1\rangle \tag{1.9}$$

where, $\phi_2 - \phi_1 = \phi$ is the relative phase of coefficients. One can easily visualize that the normalization condition leads us to the equation of a unit sphere in real three-dimensional space known as the Bloch sphere. The Bloch sphere representation can be used to geometrically characterize the state of a qubit where the Bloch sphere coordinates (x,y,z) for a general single qubit state ρ can be evaluated as

$$x = Tr(\rho\ \sigma_x), \qquad y = Tr(\rho\ \sigma_y), \qquad z = Tr(\rho\ \sigma_z)$$

For a pure state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, (x,y,z) are represented as $(Re(\alpha^*\beta), Im(\alpha^*\beta), |\alpha|^2 - |\beta|^2)$. Considering $|\alpha|^2 - |\beta|^2 = Cos^2(\gamma) - Sin^2(\gamma) = Cos(2\gamma)$, and comparing the set of coordinates with the spherical polar coordinates $(Sin\theta\ Cos\phi,\ \ Sin\theta\ Sin\phi,\ \ Cos\theta)$, we have $\gamma = \frac{\theta}{2}$. Therefore, angles

on the Bloch sphere can be interpreted as twice the value as they are in a Hilbert space. Hence, for geometrical representation, a single qubit pure state can also be represented as

$$|\psi\rangle = Cos\left(\frac{\theta}{2}\right)|0\rangle + e^{\iota\phi} Sin\left(\frac{\theta}{2}\right)|1\rangle \tag{1.10}$$

where θ and ϕ, for a particular value, represent a point on the three-dimensional Bloch sphere such that $0 \leq \theta \leq \pi$ and $0 \leq \phi < 2\pi$. Clearly, there are infinite such points for different values of θ and ϕ and therefore the state of a qubit can be represented in infinitely many ways. The Bloch vectors are equivalent to polarization vectors of a qubit as defined above and therefore for $|0\rangle$ and $|1\rangle$ states, the components of polarization vectors are $P_x = P_y = 0$, $P_z = 1$ and $P_x = P_y = 0$, $P_z = -1$, respectively indicating that $|0\rangle$ and $|1\rangle$ states are characterized by polarization vectors of unit magnitude oriented in $+Z$ and $-Z$ directions. Figure 1.1 further demonstrates the positioning of orthonormal basis vectors $|0\rangle$ and $|1\rangle$ and justifies the choice of angle as $\frac{\theta}{2}$ on the Bloch sphere. Similar to the Z-axis representing orientation of computational basis states, X-axis and Y-axis

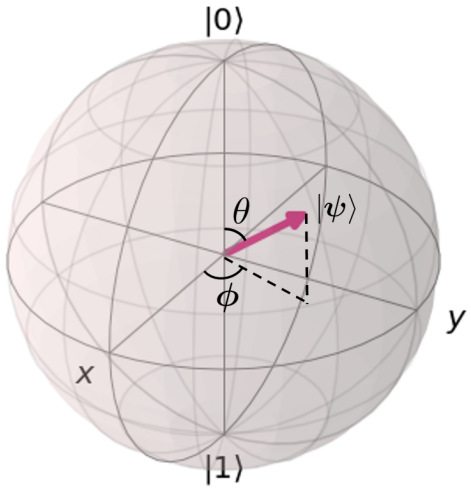

Figure 1.1 : Representation of a single qubit state on the Bloch sphere

represent superposition states for specific values of θ and ϕ as represented in the Table 1.1 and Figure 1.2. Bloch sphere further provides a way to visualize transformation of quantum states from one form to another using single qubit unitary operations [Anis *et al.*, 2021]. Moreover,

Table 1.1 : Single qubit states with corresponding angles and coordinates on the Bloch sphere

$\|\psi\rangle$	θ	ϕ	**Bloch sphere coordinates**	**Description**
$\|0\rangle$	0	-	(0,0,1)	on the positive z-axis
$\|1\rangle$	π	-	(0,0,-1)	on the negative z-axis
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{\pi}{2}$	0	(1,0,0)	on the positive x-axis
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{\pi}{2}$	π	(-1,0,0)	on the negative x-axis
$\frac{1}{\sqrt{2}}(\|0\rangle + \iota\|1\rangle)$	$\frac{\pi}{2}$	$\frac{\pi}{2}$	(0,1,0)	on the positive y-axis
$\frac{1}{\sqrt{2}}(\|0\rangle - \iota\|1\rangle)$	$\frac{\pi}{2}$	$-\frac{\pi}{2}$	(0,-1,0)	on the negative y-axis

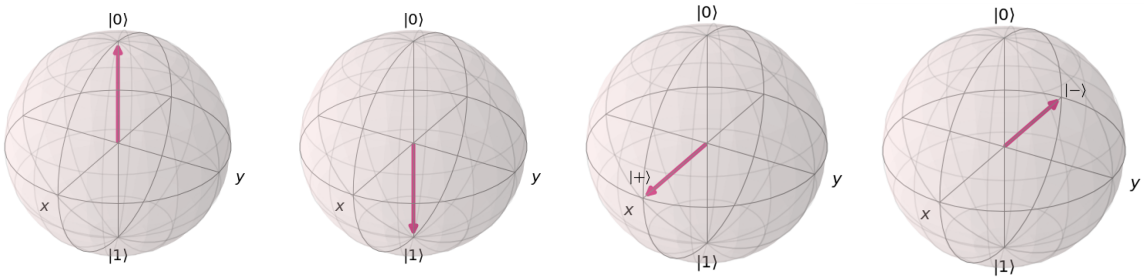

Figure 1.2 : Representations of single qubit states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ on the Bloch sphere

Bloch sphere picture can also be used to determine the purity of a state. Considering that pure states are characterized by a polarization vector of unit magnitude, pure states are represented by all points on the surface of the Bloch sphere. Similarly mixed states, having the polarization vector of less than the unit magnitude, are represented by all interior points on the Bloch sphere. For example a completely mixed state, $\frac{I}{2}$, can be represented by the center of the Bloch sphere as the state has no polarization. Hence, the purity of a state can be defined as the degree of its proximity to the surface of the sphere.

1.2.4 Multiqubit states

In order to analyze a protocol or to create a network of users in quantum information and computation, one needs to construct and characterize multiqubit systems. The quantum state of two or more than two qubits is considered as a multiqubit state. Defining a multiqubit system requires expansion of vector or Hilbert space associate with individual qubits to construct a composite vector or Hilbert space. The composite vector space for a multiqubit system can be realized using direct product of individual vector spaces. For example, if we have two individual vector spaces V_1 and V_2, then the composite vector space V can be described as $V = V_1 \otimes V_2$. This definition can similarly be extended to a quantum system composed of N qubits. For simplicity, here, we only emphasize on the process for a two-qubit state. For this, let us assume that individual states of two qubits are defined as $|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$ and $|\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$ where individual vector spaces are spanned by $|0\rangle, |1\rangle$ vectors, then a general two-qubit state can be defined using the tensor product or Kronecker product of individual qubits as

$$|\psi_{12}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix} \otimes \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \begin{bmatrix} \alpha_1 \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \\ \beta_1 \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix} \tag{1.11}$$

Here the vector space of the two-qubit system is spanned by $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. More generally, the state of a two-qubit system is defined as

$$|\psi_{12}\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} \tag{1.12}$$

such that the normalization condition requires $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. If one performs a measurement on the state of a two-qubit system, the possible measurement outcomes $|ij\rangle$ occur with respective probabilities $|\alpha_{ij}|^2$ where $i, j \in \{0, 1\}$. Owing to the superposition principle, all the four basis states can be represented as a linear superposition and can be stored in form of a single state vector. The inherent linearity of quantum theory further allows one to perform the same operation on all four basis states simultaneously in a single step. We can extend this discussion to

an N qubit state comprising of 2^N basis states and expressed as

$$|\psi_n\rangle = \sum_{i_1 \ldots i_n \in \{0,1\}} \alpha_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle \tag{1.13}$$

which, in vector representation, is a unit vector of 2^n dimensions with normalization condition requiring $\sum_{i_1 \ldots i_n \in \{0,1\}} |\alpha_{i_1 \ldots i_n}|^2 = 1$. This seems incredible as one can represent all 2^N basis states using a single quantum register. A quantum computer can therefore perform the same operation on all 2^N basis states in one single step which would require a classical computer to either perform 2^N operations or let 2^N processors working in parallel. Such a simulation of a quantum computer is improbable as with the increase in number of qubits the complexity in system also increases and this further leads to exponential increase in time and space which cannot be matched up even by the best of classical resources. Therefore, in comparison to classical resources, quantum parallelism is considered as one of the reasons for the natural speed and time advantage. Apart from establishing the network and speed and memory advantage, multiqubit states also pave the way for phenomena such as quantum entanglement and nonlocality as discussed in next subsections.

1.2.5 Entanglement

With the advent of quantum theory, the first few decades of twentieth century witnessed an intense and intellectual debate to understand, analyze and accept the need of a new theory to describe properties and dynamics of microscopic systems. The revolutionary theory was put on the pedestal in form of Matrix mechanics by Heisenberg and in form of wave mechanics by Schrödinger which were later established to be an equivalent description of quantum systems. In 1927, Heisenberg demonstrated a thought experiment to show the impossibility of precisely measuring canonically conjugate variables such as position and momentum- the uncertainty principle. The proposal was in stark contrast with classical mechanics where both position and momentum of a particle can be precisely defined. This uncertainty in quantum theory is a characteristic feature of theory itself and cannot be eliminated by improving the experimental set-up in any possible manner to measure complimentary properties of a system. The uncertainty principle and statistical nature of quantum theory puzzled many physicists, and in 1935 Einstein with Podolsky and Rosen proposed another thought experiment to comprehend quantum mechanics as an incomplete physical theory [Einstein *et al.*, 1935]. They further advocated for local hidden variable theories consistent with the assumptions of locality and realism. Erwing Schrödinger first coined the word entanglement to define the counterintuitive nature of quantum theory as against the macroscopic world [Schrödinger, 1935]. David Bohm [Bohm, 1951; Bohm and Aharonov, 1957; Bohm and Hiley, 1993] further demonstrated the characteristics of entangled systems using the anti-symmetric singlet state composed of two spin particles, now known as EPR or Bell state for historic reasons. Following the discussions on quantum versus local realistic theories, John S. Bell- borrowing the hypothesis of Einstein, Podolsky and Rosen- proposed the most celebrated inequality, the Bell inequality, which must be satisfied by systems whose correlations are not spatially extended and hence can be explained by local realistic theories [Bell, 1964]. Interestingly, the inequality is violated by all two-qubit pure entangled states suggesting either one or both assumptions laying the foundations of EPR argument to be incorrect.

Algebraically, if none of the subsystems of a composite system can be described by individual state vectors then the composite system can be considered as an entangled system. The joint composite system can be described by a single state vector but the individual components can only be described by mixed state density operators. For example, let us consider two subsystems denotes as ϕ_A and ϕ_B spanned by basis vectors $|u_i\rangle$ and $|u_j\rangle$, respectively. Clearly the initial state of the joint system much before the subsystems interact with one another can be represented by

$$|\psi_{in}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle \tag{1.14}$$

Assuming the subsystems to interact and evolve in time under a time evolution operator represented in the composite Hilbert space, quantum theory predicts the state of the evolved system to be

$$|\psi_{out}\rangle = \sum_{ij} \alpha(i,j)\,|u_i\rangle\,|u_j\rangle \tag{1.15}$$

where the probability amplitude α is now associated to variables of both subsystems forming the composite space. Hence the final state cannot be written in form of state vectors of individual subsystems as $\alpha(i,j) \neq \alpha(i)\alpha(j)$. Alternately, if a composite quantum system of two or more subsystems cannot be factored as a product of its subsystems, then it is called entangled, e.g., a quantum system composed of two particles is said to be entangled if

$$|\psi_{12}\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \tag{1.16}$$

or in terms of density operators if

$$\rho_{12} \neq \rho_1 \otimes \rho_2 \tag{1.17}$$

The most celebrated set among all entangled states are probably the two-qubit maximally entangled Bell states, namely

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{1.18}$$

Quantum entanglement- the characteristic trait of quantum mechanics- has been the cynosure for decades paving a way to address foundations of quantum theory and to propose technological advancement in quantum information and computation. In the last three decades, properties of entangled resources have been utilized to propose and establish interesting and efficient concepts which are either not possible using classical resources or the efficiencies are way too better than classical resources. For example, entangled resources shared between differed users lead to seminal concepts such as dense coding [Bennett and Wiesner, 1992], quantum teleportation [Bennett *et al.*, 1993], quantum secret sharing [Hillery *et al.*, 1999], quantum computing [Bennett and DiVincenzo, 2000], quantum cryptography [Gisin *et al.*, 2002] and quantum biology [Ball, 2011; Lambert *et al.*, 2013], to name a few. In most of the cases, two-qubit maximally entangled Bell states have played a key role as resources [Bennett and Brassard, 1984; Ekert, 1991; Bennett and Wiesner, 1992; Bennett *et al.*, 1993; Zukowski *et al.*, 1993; Bouwmeester *et al.*, 1997; Hillery *et al.*, 1999; Jennewein *et al.*, 2000; Terhal *et al.*, 2001; Kim *et al.*, 2001c; Gisin *et al.*, 2002; Boström and Felbinger, 2002; Li *et al.*, 2003; Barrett *et al.*, 2004; Riebe *et al.*, 2004a; Ursin *et al.*, 2004, 2007; Gao, 2008; Shi *et al.*, 2011; Yan *et al.*, 2018; Wu *et al.*, 2021]. Apart from two-qubit maximally entangled states, multiqubit states have also been successfully utilized for innovative applications of diverse nature in quantum information and computation [Biham *et al.*, 1996; Townsend, 1997; Karlsson and Bourennane, 1998; Bose *et al.*, 1998; Huelga *et al.*, 2001; Jing *et al.*, 2003; Wei-Xing *et al.*, 2007; Liu *et al.*, 2010; Yi and Wang, 2011; Zha *et al.*, 2013; Espoukeh and Pedram, 2014; Li *et al.*, 2016b,a; Hamdoun and Sagheer, 2020; Chen *et al.*, 2020; Zhong *et al.*, 2021].

The maximally entangled states, however, are not the most general set of states one may encounter in quantum information and computation. For example, one may have to deal with non-maximally or partially entangled states [Bennett *et al.*, 1996a] such as

$$|\psi\rangle_{AB} = Cos(\theta)\,|00\rangle + e^{\iota\delta} Sin(\theta)\,|11\rangle \tag{1.19}$$

where δ is the relative phase. In terms of efficacy, it is always beneficial to deal with maximally entangled states in ideal conditions. However, in presence of noise, a pure entangled state evolves into a mixed entangled state [Kurucz *et al.*, 2001; Gour, 2004; Mozes *et al.*, 2005; Gordon

and Rigolin, 2010; Cai *et al.*, 2014] such that the nature of quantum system becomes much more intricate and one may need to further analyze efficacy of the entangled state to understand its usefulness as the input resource [Yeo, 2008; Hu *et al.*, 2010; Espoukeh and Pedram, 2014; Knoll *et al.*, 2014; Sharma and Pandey, 2015; Fortes and Rigolin, 2015; Zhou *et al.*, 2021]. Therefore, classification and quantification of entanglement and their usefulness in real conditions are of immense value [Bruß, 2002; Kreis and van Loock, 2012; Buscemi and Bordone, 2013; Tchoffo *et al.*, 2016; Singh and Kumar, 2018a,b; Arthur *et al.*, 2018; Rosario *et al.*, 2021]. A lot of effort has been devoted to understand entanglement properties of bi-partite and multiqubit systems. Although, the properties of two-qubit entangled pure states are well established, the academic community still needs a deeper understanding of entanglement and correlations in two-qubit mixed states and higher dimensional systems [Canosa and Rossignoli, 2004; Verstraete *et al.*, 2004a; Hayden *et al.*, 2006; Wang *et al.*, 2006; Datta and Vidal, 2007; Hassan, 2009; Myers and Wu, 2010; Girolami *et al.*, 2011; Galve *et al.*, 2011; Horst *et al.*, 2013; Mani *et al.*, 2015; Eltschka and Siewert, 2018]. In general, for a quantifier to be accepted as an entanglement measure- entanglement monotone- it must satisfy certain conditions [Vidal, 2000; Gingrich, 2002]. The simple generalization of two-qubit entanglement measures to multiqubit measures is not straightforward due to increased complexity as we move from a two-qubit system to a multiqubit system. The increased complexity further forces classification and quantification of pure and mixed multiqubit states highly intricate and interesting due to the challenges involved [Brandao, 2005; Rigolin *et al.*, 2006; Eltschka and Siewert, 2014].

As discussed above, there are several measures to classify and quantify entanglement in two-qubit and multiqubit states to take informed decisions towards applicability of entangled resources in quantum information and computation. Here, we describe some of the important measures used or discussed in this Thesis.

1. **Entropy of entanglement:** The degree of entanglement of a pure two-qubit state represented in Eq. (1.19) can be measured by its entropy of entanglement [Bennett *et al.*, 1996a; Wootters, 1998, 2001; Vedral, 2002], also known as entanglement of formation (Eof), which is defined as the von-Neumann entropy of either of the subsystems ρ_A or ρ_B considered alone such that

$$E(|\psi_{AB}\rangle) = S(\rho_A) = S(\rho_B). \tag{1.20}$$

Here $S(\rho) = -Tr(\rho\ log\rho)$ is the von-Neumann entropy, and ρ_A, and ρ_B represent reduced density operators associated with the individual subsystems. One can easily evaluate that the value of $E(|\psi_{AB}\rangle)$ increases from 0 to 1 for product states to maximally entangled pure states, respectively. Clearly if the input state is a product state of subsystems such that the individual subsystems can be defined by individual state vectors, i.e., the individual states are pure states then considering the pure states to be states with maximal information, the entropy associated with such subsystems will be zero; and therefore the entanglement of formation is also zero. On the other hand, if the input state is an entangled state then subsystems cannot be assigned individual state vectors; and therefore the individual subsystems are in a mixed state. Since mixed states are states with less than the maximal information- there is always a degree of uncertainty associated with them- and thus the entropy of individual subsystems is always greater than 0; and hence the entanglement of formation is also greater than zero. Obviously the entropy and therefore the entanglement of formation is unity for a maximally entangled input state as it leads to maximally mixed subsystems. For a two-qubit mixed state, entanglement of formation requires minimization over pure state decomposition of the mixed state density operator ρ such that

$$E(\rho) = min \sum_j p_j E(\psi_j). \tag{1.21}$$

The minimization procedure involved here makes the evaluation of entanglement of

formation relatively complicated in comparison to pure states [Hill and Wootters, 1997; Vedral *et al.*, 1997b; Wootters, 1998].

2. **Concurrence:** The entanglement of formation can be considered as one of the simplest measure to quantify degree of entanglement in a two-qubit state, however, for mixed states the procedure to evaluate entanglement of formation is extremely difficult. Alternately, one can evaluate degree of entanglement in two-qubit pure and mixed states using concurrence as an entanglement measure [Hill and Wootters, 1997; Wootters, 1998, 2001]. The concurrence for a two-qubit pure state can be defined as

$$C(|\psi_{AB}\rangle) = |\langle\psi_{AB}|\widetilde{\psi}_{AB}\rangle| \tag{1.22}$$

where

$$|\widetilde{\psi}\rangle = \sigma_y^{\otimes n}|\psi^*\rangle \tag{1.23}$$

and $|\psi^*\rangle$ represents complex conjugate of $|\psi\rangle$. The above definition involves spin flip transformations, σ_y, applied to all qubits of the underlying state. One can visualize that for a product state, the spin flip operations will generate orthogonal state to the original and therefore the concurrence will be 0. Similarly, a maximally entangled state, such as a two-qubit anti-symmetric singlet state, remains invariant under spin-flip operations except for a global phase factor and therefore the concurrence is unity. Similar to entanglement of formation, the value of concurrence also monotonically increases from 0 to 1 for product states to maximally entangled states, respectively. Any intermediate value of concurrence would correspond to a non-maximally entangled two-qubit state. For example, the concurrence of an arbitrary two-qubit state represented in Eq. (1.19) is $Sin2\theta$. The definition can be generalized for all two qubit states such that

$$C(\rho) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\} \tag{1.24}$$

where

$$\widetilde{\rho} = \sigma_y^{\otimes n}\,\rho^*\sigma_y^{\otimes n}. \tag{1.25}$$

and ρ^* is complex conjugate of ρ. Here λ_i's are square roots of eigen values of the operator $\rho\widetilde{\rho}$ in decreasing order. For example, a two-qubit mixed state represented as $\rho = (1-p)|00\rangle\langle 00| + \frac{p}{\sqrt{2}}|00+11\rangle\langle 00+11|$ is entangled if $p > 0$. Similarly, for a general two-qubit state given in Eq. (1.12), concurrence is 0 if $\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}$. Clearly, for a two-qubit state to be entangled, $\alpha_{00}\alpha_{11} \neq \alpha_{01}\alpha_{10}$. For two-qubit mixed states concurrence turns out to be a relatively simple measure to evaluate the degree of entanglement in comparison to entanglement of formation.

3. **Negativity:** Another useful measure to quantify degree of entanglement in two-qubit systems is negativity [Vidal and Werner, 2002; Miranowicz and Grudka, 2004] which is a measure based on the celebrated Peres–Horodecki criterion [Peres, 1996b; Horodecki, 1997]. The negativity for a two-qubit state is defined as

$$N(\rho) = -2\sum_i min\{0, \lambda_i\} \tag{1.26}$$

where λ_i's are negative eigenvalues of partial transpose matrix ρ^{T_A} with respect to the subsystem A of the density matrix ρ of composite system. Negativity as a measure is useful for pure as well as mixed two qubit states, and it can also be generalized to n-qubit states [Hofmann *et al.*, 2014; Ciampini *et al.*, 2017].

In addition to the above discussed measures for two qubit states, there are several other significant measures which define entanglement in bi-partite states such as relative entropy [Vedral *et al.*, 1997b,a; Vedral and Plenio, 1998; Vedral, 2002], distillable and bound entanglement [Bennett *et al.*, 1996c; Horodecki *et al.*, 1997, 1998; Rains, 1999; Acín, 2001; Shor *et al.*, 2001, 2003; Kaneda *et al.*, 2012; Tuncer *et al.*, 2019; Bergh and Gärttner, 2021], entanglement witnesses [Lewenstein *et al.*, 2000; Tóth, 2005; Gühne and Lütkenhaus, 2006; Eisert *et al.*, 2007; Chruściński and Sarbicki, 2014; Chruściński *et al.*, 2018; Sen *et al.*, 2021; Wang and Zheng, 2021], and positive partial transpose [Peres, 1996b; Horodecki, 1997; Giedke *et al.*, 2001; Audenaert *et al.*, 2003].

4. **Residual entanglement:** The degree of entanglement in bi-partite systems can be analyzed using above criteria to study entanglement properties of two qubits. The characterization of entanglement properties in multiqubit system is much more challenging. For example, three-qubit pure entangled systems can be classified into two inequivalent classes, namely Greenberger-Horne-Zeilinger (GHZ) class and W class [Dür *et al.*, 2000]. Dür *et al.* have shown that the set of states in two inequivalent classes cannot be transformed into one another by performing any number of local operations assisted with classical communications (LOCC). Moreover, any three-qubit pure state can be demonstrated to belong to either one of the classes by performing stochastic local operations and classical communications (SLOCC). Interestingly, one of the most celebrated entanglement measures for three-qubit GHZ class states cannot be used for W class states [Coffman *et al.*, 2000]. Therefore, the degree of entanglement in W class is being measured using different entanglement measures. The complex nature of entangled systems increased further as we move to higher number of qubits or start dealing with mixed states.

   There are several measure available for multiqubit systems as discussed above, and one such measure is known as *residual entanglement* which makes use of concurrence given in Eq. (1.24) as part of its definition to quantify entanglement in multiqubit systems. For three-qubit systems, the residual entanglement is known as *three-tangle* (τ), proposed by Coffman *et al.* [Coffman *et al.*, 2000], and defined as

$$\tau(A:B:C) = \tau(A:BC) - \tau(A:B) - \tau(A:C) \tag{1.27}$$

   where $\tau(i:j)$ represents two-tangle evaluated as square of concurrence $C(\rho_{ij})$, and the concurrence for case $(A:BC)$ is simply $2\sqrt{det(\rho_A)}$. One can further interpret $\tau(A:BC)$ as amount of entanglement between qubit A and qubits BC taken together as a single entity which bounds amount of entanglement qubit A shares with qubits B and C individually. The three-tangle is established as an excellent measure for GHZ class states [Greenberger *et al.*, 1989; Coffman *et al.*, 2000], and remains invariant against perturbation of qubit indices. For a general three-qubit GHZ class state $|\psi\rangle_{GHZ} = cos\theta\,|000\rangle + sing\theta\,|111\rangle$, $\tau = sin^2 2\theta$ suggesting that τ varies from 0 for product states to 1 for the maximally entangled state. However, evaluation of three-tangle for W class of states, $|\psi\rangle_W = a\,|001\rangle + b\,|010\rangle + c\,|100\rangle$ [Eltschka *et al.*, 2008], leads to $\tau(A:BC) = \tau(A:B) + \tau(A:C)$ and hence results in the value 0. The properties of W class of states are therefore strikingly different from that of GHZ class of states. For example, W-class is robust against the loss of a single qubit, i.e., if we trace out one of three qubits then the state of remaining two qubits is still entangled. Whereas, GHZ class will result in fully separable states after tracing out any one of the qubits. Therefore, to identify the entanglement of W-class of states, Emary and Beenakker [Emary and Beenakker, 2004] proposed another three-qubit measure to quantify entanglement in three-qubit pure states, defined as

$$\sigma = min\left(\frac{C^2_{i(jk)} + C^2_{j(ik)}}{2} - C^2_{ij}\right) \tag{1.28}$$

where the minimization is over permutations i, j, k of three subsystems of the state. Both measures- σ and τ- are used to study entanglement properties of three-qubit pure states; while τ detects entanglement in *GHZ* class of states only, σ detects entanglement in both *W* and *GHZ* classes. For the maximally entangled *GHZ* state, $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, we have $\tau = \sigma = 1$; and for the standard three-qubit *W* state, $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$, the only nonzero value is obtained for σ such that $\sigma = \frac{4}{9}$.

For a more general three-qubit state $|\psi\rangle = a_{000}|000\rangle + a_{001}|001\rangle + ... + a_{111}|111\rangle$, another equivalent expression [Coffman *et al.*, 2000] of three-tangle in terms of coefficients a_{ijk} is given by

$$\tau_3 = 2\left|\sum a_{ijk}a_{i'j'm}a_{npk'}a_{n'p'm'} \times \varepsilon_{ii'}\varepsilon_{jj'}\varepsilon_{kk'}\varepsilon_{mm'}\varepsilon_{nn'}\varepsilon_{pp'}\right| \tag{1.29}$$

where the sum is over all indices and a_{ijk} are coefficients of orthonormal basis states $|ijk\rangle$. This definition of three-tangle is further generalized to n-tangle [Wong and Christensen, 2001] as

$$\begin{aligned}\tau_n =& 2\Big|\sum a_{\alpha_1\ldots\alpha_n}a_{\beta_1\ldots\beta_n}a_{\gamma_1\ldots\gamma_n}a_{\delta_1\ldots\delta_n} \\ &\times \varepsilon_{\alpha_1\beta_1}\varepsilon_{\alpha_2\beta_2}\ldots\varepsilon_{\alpha_{n-1}\beta_{n-1}}\varepsilon_{\gamma_1\delta_1}\varepsilon_{\gamma_2\delta_2}\ldots\varepsilon_{\gamma_{n-1}\delta_{n-1}}\varepsilon_{\alpha n\gamma_n}\varepsilon_{\beta_n\delta_n}\Big|\end{aligned} \tag{1.30}$$

Although the definition of three-tangle is invariant under permutations over qubits, the generalized n-tangle is invariant under permutations of qubits only if n is even. However, for odd n if $n > 3$, the generalized definition is not invariant under permutations. Hence, for odd number of qubits with $n > 3$, the expression of n-tangle given in Eq. (1.30) can not be utilized as an effective measure. Dafa Li [Li, 2012] then proposed a more generalized form of n-tangle defined as

$$\tau_n = \frac{1}{n}\sum_{i=1}^{n}\tau_n^{(i)} \tag{1.31}$$

where

$$\begin{aligned}\tau_n^{(i)} =& 2\Big|\sum a_{\alpha_1\ldots\alpha_n}a_{\beta_1\ldots\beta_n}a_{\gamma_1\ldots\gamma_n}a_{\delta_1\ldots\delta_n} \times \varepsilon_{\alpha_i\gamma_i}\varepsilon_{\beta_i\delta_i} \\ &\times \varepsilon_{\alpha_1\beta_1}\ldots\varepsilon_{\alpha_{i-1}\beta_{i-1}}\varepsilon_{\alpha_{i+1}\beta_{i+1}}\ldots\varepsilon_{\alpha_n\beta_n} \times \varepsilon_{\gamma_1\delta_1}\ldots\varepsilon_{\gamma_{i-1}\delta_{i-1}}\varepsilon_{\gamma_{i+1}\delta_{i+1}}\ldots\varepsilon_{\gamma_n\delta_n}\Big|\end{aligned} \tag{1.32}$$

The above definition of $\tau_n^{(i)}$ for $n \geq 5$ is invariant under any permutation except for the ith qubit. Hence, Eq. (1.31) can now be used to identify entanglement of any n-qubit pure state. There are some other significant measures of entanglement for pure states of multiqubit systems available in the literature [Meyer and Wallach, 2002; Brennen, 2003; Pan *et al.*, 2004; Love *et al.*, 2007; Bai *et al.*, 2007].

5. **Multipartite negativity:** An n-qubit system is considered as a genuine multiqubit entangled system if it is not separable with respect to any of the possible bi-partitions of its n subsystems. The multiqubit entanglement of any system can thus be identified by considering all possible bi-partitions of the whole system and then calculating their negativity. Hence, for an n-qubit state ρ_n, n-partite generalization of negativity is provided by Ciampini *et al.* [Ciampini *et al.*, 2017] as

$$N(\rho_n) = \sqrt[n]{\prod_{\sigma} N(\sigma|\sigma')} \tag{1.33}$$

where $N(\sigma|\sigma')$ is the negativity as given in Eq. (1.26) of partially transposed density matrix $\rho_n^{T_\sigma}$ with respect to the partition σ, and the product in Eq. (1.33) covers all possible

bi-partitions, i.e., $\sigma|\sigma'$ of the n-qubit state ρ_n. On similar lines, the tripartite negativity [Sabín and García-Alcaine, 2008] to identify the entanglement in three-qubit systems is given as

$$N_{ABC}(\rho) = \sqrt[3]{N_{A-BC}N_{B-AC}N_{C-AB}} \tag{1.34}$$

where $N_{I-JK} = -2\sum_i min\{0,\lambda_i\}$, and λ_i are negative eigenvalues of partially transposed density operator ρ^{T_I} which is a partial transpose operator with respect to partition I, with $I = A,B,C$, and $JK = BC,AC,AB$.

Considering entanglement to be one of the most important ingredients in quantum information and computation, apart from theoretical quest to classify and quantify entanglement properties, a lot of efforts have been devoted towards experimental realization of two-qubit [Alley and Shih, 1986; Shih and Alley, 1988; Kiess *et al.*, 1993; Kwiat *et al.*, 1995; Hagley *et al.*, 1997; Kwiat *et al.*, 1999; Kim *et al.*, 2001b,a; Vasilyev *et al.*, 2017; Gonzales *et al.*, 2019; Egger *et al.*, 2019; Grimaudo *et al.*, 2020], three-qubit [Laflamme *et al.*, 1998; Bouwmeester *et al.*, 1999; Guo and Zhang, 2002; Aoki *et al.*, 2003; Gühne and Hyllus, 2003; Eibl *et al.*, 2004; Roos *et al.*, 2004; Neeley *et al.*, 2010; Lu *et al.*, 2011; Singh *et al.*, 2018; Tsujimoto *et al.*, 2018; Scheie *et al.*, 2021] and multiqubit entangled states [Sackett *et al.*, 2000; Rauschenbeutel *et al.*, 2000; Zheng, 2001; Guo *et al.*, 2002; Wu *et al.*, 2004; Su *et al.*, 2007; Gühne *et al.*, 2007; Friis *et al.*, 2019; Erhard *et al.*, 2020; Valencia *et al.*, 2020].

1.2.6 Nonlocality

In 1935, Einstein, Podolsky, and Rosen (EPR)- puzzled by the statistical nature of quantum mechanics- argued regarding lack of completeness of quantum mechanics in light of locality and realism [Einstein *et al.*, 1935]. As part of their proposal they demonstrated a thought experiment, now known as the EPR paradox, in which they considered a composite quantum state of two spin-$\frac{1}{2}$ particles such that the sum of their positions and difference of their momentum are both precisely defined. Uncertainty principle, on the other hand, advocates the impossibility of precisely defining individual momentum and position of both particles. Considering the commutator of $x_1 + x_2$ and $p_1 - p_2$ where x_i and p_i correspond to individual position and momentum of two particles, one can easily visualize that $[x_1 + x_2, p_1 - p_2] = 0$ and hence the joint properties of two particles can be precisely defined. EPR therefore concluded that a measurement to determine the position or the momentum on any one of the particles will immediately reveal the position or the momentum of the other particle without performing a measurement on the other particle or without interacting with that particle in any possible manner. Assuming that two particles are separated by an arbitrary distance, EPR suggested that the measurement on one particle cannot have any influence on properties of the other particle according to the principle of locality which suggests that an object is affected only by its neighboring objects and distant objects cannot directly effect each others properties. As a result, properties of the second particle must be independent of measurements performed on the first particle. EPR, therefore, advocated that both position and momentum of the other particle can be simultaneously known- this would clearly be in contrast to the foundations of quantum mechanics, i.e., the uncertainty principle- and since quantum mechanics cannot predict that, it is an incomplete theory. EPR further argued the possibility of existence of some physical variables- hidden variables, not known at that time- which may allow the theory to define definite properties of particles irrespective of whether we observe them or not. On these lines, EPR raised the question of completeness of quantum mechanics as a complete theory and suggested that quantum mechanical predictions are valid only if there exists some hidden variables. In a response to the raised question, Niels Bohr [Bohr, 1935] countered the argument by suggesting that two spin-$\frac{1}{2}$ particles considered in the EPR paradox are always a part of the single quantum system, and hence measurements performed on one of the subsystems always influence the predictions for the other subsystem by changing the predictions that can be obtained for the composite system, implying the completeness of quantum mechanics without the need of hidden variables. Further to Bohr's argument, several highly significant contributions were made to comprehend

that hidden-variable theories are incompatible with predictions of quantum mechanics [Jauch and Piron, 1963; Bell, 1966; Bohm and Bub, 1966, 1968; Jauch and Piron, 1968; Gudder, 1968; Gleason, 1975; Kochen and Specker, 1975]. In one of the most seminal contributions, John Bell proposed a theorem [Bell, 1964] providing the theoretical premise for the study of nonlocal correlations. The Bell inequality was derived using two basic assumptions, i.e.,
1. *Locality*: an object is affected only by its neighboring objects as distant objects cannot directly affect each other.
2. *Realism*: all the objects have definite values prior to measurement regardless of whether they are observed or not.

Using the inequality, John S. Bell proved that if principles of locality and realism are valid, then there is an upper limit to the correlations of distant events independent of any specific physical theory (i.e., the hidden variable theory), and that any hidden variable quantum theory applied to a quantum system consisting of distant subsystems must be separable. The Bell inequality clearly demarcates a boundary between correlations that can be explained using classical theories as against the correlations which are otherwise counterintuitive to our experience of the macroscopic world and that are known as nonlocal correlations. The Bell inequality is shown to be violated by all two-qubit pure entangled states and by several classes of mixed entangled states indicating that either one or both the assumptions advocated by EPR are not correct [Gisin, 1991; Popescu and Rohrlich, 1992; Gisin and Peres, 1992; Braunstein *et al.*, 1992; Horodecki *et al.*, 1995; Weihs *et al.*, 1998; Rowe *et al.*, 2001]. We will further discuss two-qubit and multiqubit nonlocality in detail in Section 1.5.

Contrary to the *principle of locality*, *nonlocality* describes the ability of distant objects to influence properties of other objects which are indeed part of a composite system. Considering the importance of entanglement and nonlocality, several studies have been devoted to study entanglement and nonlocal properties using different measures and Bell-type inequalities. Initially, nonlocal correlations were only portrayed in light of entangled systems assuming that the necessary space and time advantage offered by quantum computation is due to entangled resources only. The phenomenon of nonlocality without entanglement was first addressed by Bennett *et al.* [Bennett *et al.*, 1999], where they proposed a set of locally indistinguishable orthogonal product bases in three-dimensional Hilbert space. They further showed the non existence of any two-level pure state that may be separable but still possessing nonlocal correlations. Unlike the two-qubit pure states, there are several instances of two-qubit mixed states which are separable but still exhibit nonlocal correlations between qubits [Werner, 1989; Horodecki *et al.*, 1996; Munro *et al.*, 2001b; Gisin, 1996a; Cohen, 1998]. Moreover, the issue of existence of nonlocality with entangled systems only was further addressed by identification and application of efficient separable systems possessing quantum correlations [Dakić *et al.*, 2010; Merali, 2011; Xi *et al.*, 2012; Shi *et al.*, 2012; Gheorghiu *et al.*, 2015; Liu *et al.*, 2015; Namkung *et al.*, 2015; Chuan-Mei *et al.*, 2015; Mahdian and Arjmandi, 2016; Gerasev and Kuznetsova, 2016; Moreva *et al.*, 2017; Vedral, 2017; De Chiara and Sanpera, 2017; Bera *et al.*, 2017; Christ and Hinrichsen, 2017; Xie *et al.*, 2017; Braun *et al.*, 2017; Domínguez-Serna *et al.*, 2017; Zhang *et al.*, 2017; Zalys-Geller *et al.*, 2018; Korolkova and Leuchs, 2019; Lahlou *et al.*, 2020; Raj *et al.*, 2021]. The Bell inequality fails to identify nonlocal correlations in some mixed entangled states and separable systems; and therefore the need for defining measures which can successfully capture nonlocal correlations in mixed entangled states and separable systems. Quantum discord is one measure that captures quantumness of correlations in separable as well as entangled systems [Ollivier and Zurek, 2001; Henderson and Vedral, 2001]- the measure detects nonlocality in bi-partite systems beyond the boundaries of entanglement and Bell inequalities. Therefore, separable states having zero entanglement can still have non-zero discord suggesting their importance as resources in quantum information and computation. Discord successfully identifies quantum correlations in all non-classical systems, and can be defined as the difference between quantum mechanical analogue of two classically equivalent definitions of

mutual information. For example, quantum discord of a state ρ_{AB} is defined as a difference between the following two classically equivalent definitions of mutual information, namely

$$D_A(\rho_{AB}) = I(\rho_{AB}) - \max_{\{\Pi_j^A\}} J_{\{\Pi_i^A\}}(\rho_{AB}) \tag{1.35}$$

where $I(\rho_{AB})$ is mutual information representing total correlations between two subsystems and $J_A(\rho_{AB})$ is measurement based mutual information representing only the classical correlations between two subsystems, given by

$$\begin{aligned} I(\rho_{AB}) &= S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \\ J_A(\rho_{AB}) &= S(\rho_B) - S(\rho_B|\rho_A) \end{aligned} \tag{1.36}$$

Here $S(\rho_A)$ and $S(\rho_B)$ are the von-Neumann entropy of subsystems A and B respectively, $S(\rho_{AB})$ is von-Neumann entropy of the joint system AB and $S(\rho_B|\rho_A)$ is the conditional quantum entropy. Although quantum discord is an excellent measure of nonlocal correlations in quantum states, the optimization procedure involved makes its evaluation rather difficult [Luo, 2008; Girolami and Adesso, 2011; Chen *et al.*, 2011; Huang, 2014]. Considering the importance of quantumness of correlations, a simplified geometric measure was proposed [Dakić *et al.*, 2010], i.e,

$$D_G(\rho_{AB}) = \min_{\{\chi \in \Omega_0\}} ||\rho_{AB} - \chi||^2 \tag{1.37}$$

where Ω_0 denotes the set of zero-discord states and $||A-B||$ is the Hilbert–Schmidt norm. Further a two-qubit density operator in the Bloch representation is

$$\rho_{AB} = \frac{1}{4}\left[I_4 + \sum_{i=1}^{3} x_i I_2 \otimes \sigma_i + \sum_{i=1}^{3} y_i \sigma_i \otimes I_2 + \sum_{i,j=1}^{3} t_{ij}\sigma_i \otimes \sigma_j\right] \tag{1.38}$$

where $x_i = Tr(\rho_{AB}(I_2 \otimes \sigma_i))$ and $y_i = Tr(\rho_{AB}(\sigma_i \otimes I_2))$ are elements of Bloch vectors X and Y; and $t_{ij} = Tr(\rho_{AB}(\sigma_i \otimes \sigma_j))$ are components of correlation matrix T. A convenient measure to capture non-classicality is further defined as quantum discord in the form of Bloch vectors (X or Y) and correlation matrix T such that

$$D_G(\rho_{AB})^{(A)} = \frac{1}{4}\left[||X||^2 + ||T||^2 - \lambda_{max}(XX^T + TT^T)\right] \tag{1.39}$$

where λ_{max} is the maximum eigenvalue of $(XX^T + TT^T)$. Both discord and geometric discord given in Eq. (1.35) and Eq. (1.39), are not symmetric with respect to the two subsystems A and B. In comparison to the original definition of discord, the geometric measure of discord is much more easier and convenient to compute analytically. However both measures, discord or geometric discord, have their own advantages and disadvantages [Piani, 2012]. Nevertheless, both these measures are extremely important as genuine measures of non-classicality and are studied in detail [Luo and Fu, 2010; Xu, 2012; Passante *et al.*, 2012; Jin *et al.*, 2012; Zhang *et al.*, 2012; Paula *et al.*, 2013; Qiang *et al.*, 2015; Chuan-Mei *et al.*, 2015; Wu and Zhou, 2015; Qiang *et al.*, 2016; Roga *et al.*, 2016; Jakóbczyk *et al.*, 2016; Hu *et al.*, 2018; Liang and Zhang, 2020; Dobre and Isar, 2020].

1.2.7 Quantum gates

In the previous subsections, in addition to representations of qubits and multiqubit states, we have also discussed characteristics and applications of entanglement and nonlocality. We now proceed to demonstrate how the information encoded in qubits can be mapped from one form to another or how does one create an entangled state using single and multiqubit quantum gates. Similar to classical computation where logic gates transform a set of inputs to the desired output, in quantum computation, input states can be mapped to desired output states using quantum

gates. However, unlike logic gates, quantum gates are reversible in nature in a sense that given an output state one can always evaluate the input state by running the required gates backward. Algebraically, the state of a qubit evolves under the operation of quantum gates to yield a new state $|\psi'\rangle$. Considering that the norm of the evolved state remains invariant under these operations, the only constraint that the theory imposes on the representation of quantum gates is for a gate to be represented by a unitary matrix. Therefore, quantum gates are represented by unitary operators, e.g., a single qubit quantum gate can be represented by a 2×2 unitary matrix U such that $UU^\dagger = U^\dagger U = I$ where I is a 2×2 identity matrix. The fact that for any quantum gate U, $U^{-1} = U^\dagger$, ensures that we can always overturn the operation of a quantum gate, i.e., a quantum gate is logically reversible.

In this subsection, we first demonstrate the importance of single qubit quantum gates and then extend our discussion for applicability of multiqubit quantum gates to create network among different users in quantum information and computation. For single qubits, one can define infinitely many 2×2 unitary matrices to be used as quantum gates. For our purpose, here we describe some of the standard single qubit gates- in fact one can decompose an arbitrary unitary operator in terms of simple single qubit unitary operations as well.

1. Identity gate: As the name suggests, an identity operator corresponding to the identity gate does not change the state of a qubit and leaves it as it is, therefore, performing an identity operation corresponds to doing nothing to the state of a qubit. Hence the actions of an identity gate are represented as
   $I|0\rangle = |0\rangle$, *and* $I|1\rangle = |1\rangle$ *or*
   $I(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle$

2. Pauli-X gate: The only exception to the irreversibility of logic gates is the non-trivial NOT gate as it is a reversible logic gate flipping the state of a bit from 0 to 1 and 1 to 0. An analogues operation- X gate- exists in quantum computation which flips the computational basis from one form to the another, i.e. the operation flips $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. Since quantum operations are linear, the action of X-gate on an arbitrary linear superposition of $|0\rangle$ and $|1\rangle$ can therefore be
   $X|\psi\rangle = X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle = |\psi'\rangle$
   Clearly, if one performs the X-gate again on the output $|\psi'\rangle$, the resultant state will be $|\psi\rangle$ representing the original input confirming the reversible nature of X-gate. Geometrically, the operation of an X-gate on the Bloch sphere is a π-rotation of computational basis states about the X-axis.

3. Pauli-Y gate: On the similar lines as discussed above, a Y-gate transforms the state $|0\rangle$ to $\iota|1\rangle$ and $|1\rangle$ to $-\iota|0\rangle$ such that
   $Y|\psi\rangle = Y(\alpha|0\rangle + \beta|1\rangle) = \alpha Y|0\rangle + \beta Y|1\rangle = \alpha(\iota|1\rangle) + \beta(-\iota|0\rangle) = \iota(\alpha|1\rangle - \beta|0\rangle) = |\psi'\rangle$
   In terms of a Bloch sphere, the operation of a Y-gate can be interpreted as rotating the computation basis states by an angle π around the Y-axis. Moreover, operating Y-gate again on the output, one can easily retrieve the input state.

4. Pauli-Z gate: The single qubit Z-gate can be used to introduce a relative phase between the computational basis states of a qubit. The gate when operates on the state $|0\rangle$ leaves it as it is but when it operates on $|1\rangle$, it imparts a negative sign to the state to yield $-|1\rangle$. In general,
   $Z|\psi\rangle = Z(\alpha|0\rangle + \beta|1\rangle) = \alpha Z|0\rangle + \beta Z|1\rangle = \alpha|0\rangle - \beta|1\rangle = |\psi'\rangle$
   From the properties of Z-gate, it is obvious that the gate is reversible. As defined earlier, the above three single qubit gates, i.e., X, Y, and Z are commonly known as the Pauli operators. These operators are also represented as σ_x, σ_y, σ_z, respectively. In addition to being unitary, the Pauli operators are also Hermitian, i.e., $\sigma_i^\dagger = \sigma_i$, and hence σ_i^2 = I. Moreover, the Pauli operators anti-commute with each other,i.e.,

$XY = -YX$
$YZ = -ZY$
$ZX = -XZ$

5. Hadamard gate: The Hadamard gate is considered as one of the most useful single qubit gates in the sense that the operation of a Hadamard gate on computational basis states allows one to create a superposition state, i.e.
$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
and
$H|\psi\rangle = H(\alpha|0\rangle + \beta|1\rangle) = \alpha H|0\rangle + \beta H|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle = |\psi'\rangle$
The operation of a Hadamard gate on an arbitrary single qubit state can be interpreted as the demonstration of interference. The H gate can also be represented as an equal superposition of X and Z gate such that $H = \frac{1}{\sqrt{2}}(X+Z)$. It is easy to evaluate $HH^\dagger = H^2 = I$, and thus operating the Hadamard gate twice on the input state will result in the original input state. Further, the operation of a Hadamard gate can be visualized as a π-rotation around the diagonal $(X+Z)$ axis.

A summary of the above single qubit operations and their matrix representations is expressed in Table 1.2. As the above discussed gates operate on a single qubit, we now proceed to discuss

Table 1.2 : Summary of single qubit gate operations

S.No.	Gate	Matrix representation	Action
1)	Identity	$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$I(\alpha\|0\rangle + \beta\|1\rangle) = \alpha\|0\rangle + \beta\|1\rangle$
2)	Pauli-X	$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$X(\alpha\|0\rangle + \beta\|1\rangle) = \alpha\|1\rangle + \beta\|0\rangle$
3)	Pauli-Y	$Y = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}$	$Y(\alpha\|0\rangle + \beta\|1\rangle) = \imath\alpha\|1\rangle - \imath\beta\|0\rangle$
4)	Pauli-Z	$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$Z(\alpha\|0\rangle + \beta\|1\rangle) = \alpha\|0\rangle - \beta\|1\rangle$
5)	Hadamard	$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$	$H(\alpha\|0\rangle + \beta\|1\rangle) = \alpha\frac{\|0\rangle+\|1\rangle}{\sqrt{2}} + \beta\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$

operations of multiqubit gates. Similar to our discussion on single qubit gates, for two-qubits also, the no-operation gate is Identity gate represented by a 4×4 identity matrix. Other than the trivial identity gate, the important two-qubit gates include controlled and SWAP gates. As the standard notation, a two-qubit controlled gate operates on a two qubit state such that one of the qubits acts as a control qubit and the second qubit acts as a target qubit in a sense that a single qubit gate is applied on the state of target qubit if the state of control qubit is set to $|1\rangle$. One of the most important controlled gate is a Controlled-NOT (C-NOT) gate where Pauli-X operation is applied on the target qubit whenever the state of control qubit is $|1\rangle$. Hence, a C-NOT gate flips the state of target qubit if and only if the state of control qubit is $|1\rangle$. Clearly, the matrix representation of a

C-NOT gate is

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{1.40}$$

Moreover, if the states of control and target qubits are represented as $|i\rangle$ and $|j\rangle$, then the actions of a C-NOT gate can also be visualized as $|i\rangle|j\rangle \rightarrow |i\rangle|j \oplus i\rangle$ where $\oplus$ represents addition modulo 2. The C-NOT gate is highly significant to quantum information and computation as it plays the role of an entangler and disentangler. For example, together with a single qubit Hadamard-gate, the CNOT gate can be used to create entanglement starting from an input two-qubit product state. In order to prepare two-qubit maximally entangled Bell states staring from product states, one needs to perform a single-qubit Hadamard gate on one of the qubits, say on the first qubit to create superposition, and then needs to perform a C-Not gate considering the second qubit as target qubit. The set of operations on different inputs to prepare four Bell states, are summarized below as

$$|0\rangle_1 \otimes |0\rangle_2 \xrightarrow{H^{(1)}} \frac{1}{\sqrt{2}}|0+1\rangle_1 \otimes |0\rangle_2 \xrightarrow{CNOT^{(1-2)}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle_{12}$$

$$|1\rangle_1 \otimes |0\rangle_2 \xrightarrow{H^{(1)}} \frac{1}{\sqrt{2}}|0-1\rangle_1 \otimes |0\rangle_2 \xrightarrow{CNOT^{(1-2)}} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\phi^-\rangle_{12}$$

$$|0\rangle_1 \otimes |1\rangle_2 \xrightarrow{H^{(1)}} \frac{1}{\sqrt{2}}|0+1\rangle_1 \otimes |1\rangle_2 \xrightarrow{CNOT^{(1-2)}} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\psi^+\rangle_{12}$$

$$|1\rangle_1 \otimes |1\rangle_2 \xrightarrow{H^{(1)}} \frac{1}{\sqrt{2}}|0-1\rangle_1 \otimes |1\rangle_2 \xrightarrow{CNOT^{(1-2)}} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\psi^-\rangle_{12}$$

here $H^{(1)}$ is the Hadamard gate applied on the state of first qubit, $CNOT^{(1-2)}$ is the controlled-NOT gate with first qubit as a control qubit and second as a target qubit, and $|\phi^{\pm}\rangle, |\psi^{\pm}\rangle$ are the four Bell states. Considering the reversible nature of quantum gates, in one further applies a C-NOT gate and then a Hadamard gate on Bell states in a similar way as discussed for creating entanglement then the Bell states get disentangled and lead to the respective product states.

Similar to the C-NOT gate, a Controlled-Z (CZ) gate is another example of a two-qubit controlled gate. As the name suggests, in this case, the Pauli-Z operation is applied on the target qubit whenever the control qubit is set to $|1\rangle$. The CZ is represented by a 4×4 unitary matrix as

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{1.41}$$

The operation of a CZ gate can be interpreted as flipping the phase of the target qubit if the control qubit is in $|1\rangle$ state. Similar to these two controlled gates, one can create many other two-qubit controlled gates by applying a single qubit gate on the target qubit depending on the state of control qubit [Ekert *et al.*, 1999, 2001; Ekert, 2002]. In a sense, these controlled gates implement *if-else* type operations, e.g., a C-NOT gate flips the target qubit *if* the control qubit is set to $|1\rangle$, *else* it does nothing.

Another important two-qubit gate is the SWAP gate which swaps the state of two-qubits when operated and therefore the matrix representation of a SWAP gate is

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{1.42}$$

In context of the physical realization of quantum computers, SWAP gates are required to shift qubits into physical proximity so that other gates can be executed between the neighboring qubits [Cheung *et al.*, 2007; Venturelli *et al.*, 2019]. SWAP operations can also be performed using C-NOT gates such that

$$SWAP^{(1-2)} = CNOT^{(1-2)}CNOT^{(2-1)}CNOT^{(1-2)} \tag{1.43}$$

where the superscript $(i-j)$ represents i as the control qubit and j as the target qubit.

The representation of two-qubit controlled gates discussed above can be generalized to have multiple controls. For example, in case of a three-qubit controlled gate, an operation is performed on the state of third qubit depending on the state of first two qubits. One such three-qubit controlled gate is the Toffoli gate, which is a quantum analogue of a reversible classical logic gate with the same name. The Toffoli gate is a two control qubits and one target qubit gate, and is also known as a controlled-controlled-NOT (or C-CNOT) gate suggesting its actions as flipping the state of target qubit if and only if the first two qubits (control qubits) are in $|1\rangle$ states. Similar to the C-NOT gate, if input states are represented as $|i\rangle\,|j\rangle$ and $|k\rangle$, then the actions of a Toffoli gate can be visualized as $|i\rangle\,|j\rangle\,|k\rangle \rightarrow |i\rangle\,|j\rangle\,|k \oplus ij\rangle$. Toffoli gate can efficiently simulate classical logic gates indicating the importance of quantum gates in terms of performing similar computations as classical computers [Toffoli, 1980; Williams *et al.*, 1998; Iqbal and Banday, 2015]. Considering the importance of quantum gates, a lot of work has been done towards experimental implementation and applications of these gates in quantum information and computation [Sleator and Weinfurter, 1995; Wei and Lei, 2000; Plantenberg *et al.*, 2007; Zu *et al.*, 2014; Zhang *et al.*, 2015; Rong *et al.*, 2015; Babazadeh *et al.*, 2017; Russ *et al.*, 2018; Huang *et al.*, 2019; Xu *et al.*, 2020b; Li *et al.*, 2021; Zhang *et al.*, 2022].

1.3 SYSTEM-ENVIRONMENT INTERACTIONS AND QUANTUM NOISE

In ideal conditions, we assume the principal quantum system to be in complete isolation such that the system of interest does not interact with its surroundings or environment. Such systems are considered as the ideal ones and are known as closed systems. However, under real conditions, the interactions between a principal quantum system and its environment are inevitable. Therefore such an isolated ideal system is a distant reality, and quantum systems do interact with environment resulting in the phenomenon termed as quantum noise or decoherence [Gardiner, 1991]. Such systems with unavoidable interplay between the system of interest and environment are known as open systems [Davies and Davies, 1976]. These interactions leading to decoherence adversely affect nonlocal correlations existing between the qubits, thereby affecting the overall efficiency of a resource or communication protocol. Hence, one needs to find mechanisms to model and characterize such interactions to understand and address its effects on quantum information and computation.

These noisy channels can be modeled by a completely positive trace preserving evolution given by $\varepsilon(\rho)$ of a density operator ρ such that $\varepsilon(\rho) = \sum_k E_k \rho E_k^\dagger$, where E_k are single qubit operational elements of the quantum noise under consideration- also known as Kraus operators- satisfying the completeness relation $\sum_k E_k^\dagger E_k = I$. In order to understand the mathematical formalism and the mechanism of how noisy channels nullify the advantages of quantum correlations, we briefly discuss quantum noises often described in terms of channels by considering their Kraus operator representations.

1. **Amplitude damping channels** describe effects due to energy loss from a quantum system, which can be a result of spontaneous emission, scattering or attenuation of a photon. The

Kraus operators or operational elements of an amplitude damping channel are

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-d} \end{bmatrix}, \qquad E_1 = \begin{bmatrix} 0 & \sqrt{d} \\ 0 & 0 \end{bmatrix} \tag{1.44}$$

2. **Phase damping channels** describe the loss of quantum information without loss of energy. Unlike the amplitude damping channel, in this case the information is lost in form of the relative phase between eigen states. The Kraus operators of the phase damping channel are

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-d} \end{bmatrix}, \qquad E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{d} \end{bmatrix} \tag{1.45}$$

3. **Depolarizing channels** map pure states to completely mixed or depolarized states. It evolves the original state to a completely mixed state with probability d and leaves the system unaltered with probability *1-d*. The evolution of the state in this case is given as

$$\mathcal{E}(\rho) = \frac{d}{2} I + (1-d)\rho, \tag{1.46}$$

and the operational elements for this channel are

$$E_0 = \sqrt{1 - \frac{3d}{4}} I, \;\; E_1 = \frac{\sqrt{d}}{2} X, \;\; E_2 = \frac{\sqrt{d}}{2} Y, \;\; E_3 = \frac{\sqrt{d}}{2} Z \tag{1.47}$$

where X, Y, Z are Pauli operators and I is 2×2 identity matrix, as given in Table 1.2.

4. **Bit flip and phase flip channels** produce Pauli gate errors. For example, the *Bit flip channel* flips the state of a qubit, i.e., $|0\rangle$ to $|1\rangle$ (and vice-versa) with probability $1-d$ and leaves the qubit unchanged with probability d. Therefore the operational elements of a bit flip channel can be summarized as

$$E_0 = \sqrt{d} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \sqrt{d}\, I, \qquad E_1 = \sqrt{1-d} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \sqrt{1-d}\, X \tag{1.48}$$

Similarly, as the name suggests, the *phase flip channel* introduces a phase if the eigenstate is represented as $|1\rangle$ with probability $1-d$ else leaves the system unaltered with probability d. The operational elements for this channel are

$$E_0 = \sqrt{d} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \sqrt{d}\, I, \qquad E_1 = \sqrt{1-d} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \sqrt{1-d}\, Z \tag{1.49}$$

The *bit-phase flip channel* is the combination of both bit flip and phase flip errors. It keeps the state of a qubit unchanged with probability d and inducts both bit and phase flip errors with probability $1-d$. The operational elements for the bit-phase flip channel are

$$E_0 = \sqrt{d} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \sqrt{d}\, I, \qquad E_1 = \sqrt{1-d} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \sqrt{1-d}\, Y \tag{1.50}$$

Quantum noise adversely affects the efficiency of a quantum system as the original system evolves with degradation of the entanglement and nonlocal correlations between qubits. The interactions with environment result in destroying coherence of quantum systems [Zurek, 2003; Unruh, 1995; Mahdian *et al.*, 2012; Kapral, 2015]. The correlations existed in quantum systems can thus be deteriorated by environmental noise in such a way the degree of entanglement in quantum systems decreases abruptly and the system loses entanglement and nonlocality

completely in a finite time scale- this sudden loss of entanglement is termed as entanglement sudden death (ESD) [Yu and Eberly, 2006; Cui *et al.*, 2007]. Recently, effect of environmental noise on quantum systems and entanglement sudden death have been studied in detail [Yu and Eberly, 2004; Almeida *et al.*, 2007; Salles *et al.*, 2008; Ann and Jaeger, 2008; Yu and Eberly, 2009]. The fact that efficacies of a communication protocol may depend on entanglement and nature of correlations, decoherence substantially impacts efficiencies of quantum systems for different quantum information processing protocols including quantum teleportation, quantum dense coding, entanglement swapping, quantum algorithms, quantum cryptography etc. [van Enk and Hirota, 2001; Rao *et al.*, 2008; He *et al.*, 2006; Prakash *et al.*, 2007; Huang *et al.*, 2017; Ban *et al.*, 2005; Dajka and Łuczka, 2013; Bettelli and Shepelyansky, 2003; Azuma, 2002; Pablo-Norman and Ruiz-Altaba, 1999; Ban *et al.*, 2006]. Therefore, the need to find mechanisms to protect entangled systems from decoherence to preserve nonlocal correlations. On these lines many decoherence models such as quantum error correcting codes [Shor, 1995; Steane, 1996; Devitt *et al.*, 2013], quantum purification [Bennett *et al.*, 1996b; Pan *et al.*, 2003], entanglement distillation [Bennett *et al.*, 1996a; Kwiat *et al.*, 2001; Dong *et al.*, 2008], quantum zeno-effect [Itano *et al.*, 1990; Maniscalco *et al.*, 2008], decoherence-free subspace [Lidar *et al.*, 1998; Kwiat *et al.*, 2000; Walton *et al.*, 2003], weak measurement and its reversal operations [Kim *et al.*, 2012; Sun *et al.*, 2010; Korotkov and Keane, 2010; Lee *et al.*, 2011a] have been used effectively in literature to protect quantum correlations between qubits. Among all these decoherence models, one that has been recently used effectively to protect quantum correlations between qubits is weak measurement and its reversal operations [Korotkov and Keane, 2010; Cheong and Lee, 2012; Paraoanu, 2006; Franco *et al.*, 2012; Katz *et al.*, 2008; Paraoanu, 2011; Lee *et al.*, 2011a; Kim *et al.*, 2012; Korotkov and Jordan, 2006; Kim *et al.*, 2009; Sun *et al.*, 2009; Xiao and Li, 2013; Sun *et al.*, 2010]. The technique is found to be a useful tool to protect entanglement, nonlocality, and efficiency of quantum systems from decoherence [Kim *et al.*, 2012, 2009; Xiao and Li, 2013; Sun *et al.*, 2009, 2010; Korotkov and Jordan, 2006; Xu *et al.*, 2013; Katz *et al.*, 2006; Groen *et al.*, 2013; Guan *et al.*, 2017; Pramanik and Majumdar, 2013; Singh and Kumar, 2018a,b; Liao *et al.*, 2021]. In comparison to the usual quantum measurement in which a quantum state irreversibly collapses to one of its eigen states, weak measurements do not collapse the state and the state of the system can actually be reversed.

In 2012, Kim *et al.* [Kim *et al.*, 2012] proposed a scheme to protect entanglement from decoherence, based on the fact that the weak measurements can be reversed. The proposed scheme demonstrates use of weak measurement and corresponding quantum measurement reversal to suppress the effect of decoherence as shown in Figure 1.3, where w is the weak measurement strength, d is decoherence parameter and w_r is the strength of reversing measurement. For an amplitude damping channel, the optimum value for reversal measurement to protect entanglement and nonlocal correlations is given as $w_r = w + d(1-w)$ [Kim *et al.*, 2012]. In order to achieve the same, one needs to perform weak measurement operations locally on each qubits before sending them through local noisy channels. Once the qubits pass through noisy channels, one needs to perform weak measurement reversal operations locally on each qubits. The evolution of the initial state or density operator ρ following the above argument is therefore given by $\varepsilon'(\rho)$ such that $\varepsilon'(\rho) = M_{rev}\left[\sum_k E_k(M_{wk}\rho M_{wk})E_k^\dagger\right]M_{rev}$, where M_{wk}, M_{rev} and E_k are weak measurement operator, weak measurement reversal operator and Kraus operators for the amplitude damping noise, respectively.

For analyzing the applications of weak measurements on quantum states, weak measurement ($M_{wk}(w)$) and corresponding reversal ($M_{rev}(w_r)$) operations are represented as

$$M_{wk}(w) = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-w} \end{bmatrix}, \qquad M_{rev}(w_r) = \begin{bmatrix} \sqrt{1-w_r} & 0 \\ 0 & 1 \end{bmatrix} \tag{1.51}$$

where $0 \leq w, w_r \leq 1$. On applications of weak measurement and reversal weak measurement operations before and after the amplitude damping noise, the final state depends on the noise

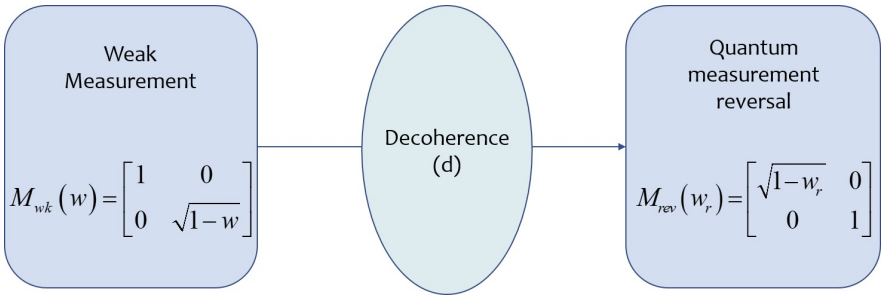

Figure 1.3 : Application of weak measurement and quantum measurement reversal in the presence of a decoherence channel

parameter, the state parameter, and weak measurement parameters. This state can therefore now be utilized for performing the quantum information processing protocols.

1.4 QUANTUM INFORMATION PROCESSING PROTOCOLS

With the advent of quantum information and computation, entanglement and nonlocal correlation have played a crucial role not only in understanding the foundational aspects of theory but also for proposing and implementing many potential applications which are otherwise not possible using classical resources, for instance- teleporting an unknown quantum state without traveling physically [Bennett *et al.*, 1993], transferring two classical bits of information by sending only one qubit form sender to receiver [Bennett and Wiesner, 1992; Barenco and Ekert, 1995], possibly unbreakable quantum key distribution [Bennett and Brassard, 1984], secretly sharing the message by splitting it into several parts [Hillery *et al.*, 1999], possibility of preserving quantum coherence in the presence of noises [Bennett *et al.*, 1996c], secure transmission of classical information [Gisin *et al.*, 2002], computational speed-up [Jozsa and Linden, 2003], to probe and control biological functions [Cai *et al.*, 2010], an entanglement-enhanced microscope [Ono *et al.*, 2013], quantum internet [Cacciapuoti *et al.*, 2019; Wang *et al.*, 2020], and efficient computations [Steane, 1998; Henriet *et al.*, 2020].

In the following subsections, we briefly discuss some of the pioneer protocols which further paved a way for significant applications in quantum information and computation.

1.4.1 Quantum teleportation

One of the most discussed phenomenon- from science fiction to reality- is quantum teleportation which allows the transfer of unknown information encoded in a quantum state from one arbitrary location to another without sending the information through any medium [Bennett *et al.*, 1993]. The term 'quantum teleportation' is defined as a quantum mechanical process which allows one to transmit information over arbitrary distances without sending the quantum information through a physical medium at any point of time, and without measuring the unknown information at either sides of transportation. The fact that no medium is required for the protocol indicates that one teleports the physical state of a qubit instead of sending the qubit itself. The teleportation of *Physical state* of a qubit, however, suffices as it contains all the information about the qubit. In order to describe the nuances of quantum teleportation, we first briefly discuss the protocol here. For successfully implementing the protocol, Alice (sender) and Bob (receiver) share an entangled state $|\Psi_{23}^{-}\rangle = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]_{23}$ such that qubit 2 belongs to Alive and qubit 3 belongs to Bob. The shared entangled state between the two users acts as a quantum channel for the teleportation protocol. Alice wants to communicate an unknown information encoded in a state $|\psi_{in}\rangle = Cos(\frac{\xi}{2})|0\rangle + e^{\imath\phi}Sin(\frac{\xi}{2})|1\rangle$ to Bob, where ξ and ϕ are polar coordinates with $0 \leq \xi \leq \pi$ and $0 \leq \phi \leq 2\pi$. For this, Alice first performs a two-qubit Bell-state measurement on the joint state of

her qubits- one from the shared entangled pair and one defining the input state, and then sends her measurement outcomes to Bob through a classical channel. The joint three-qubit state just before Alice's measurement is represented as

$$|\psi_{123}\rangle = \frac{1}{2}\Big[|\Psi_{12}^{-}\rangle\left(-Cos(\tfrac{\xi}{2})|0\rangle - e^{\iota\phi}Sin(\tfrac{\xi}{2})|1\rangle\right) + |\Psi_{12}^{+}\rangle\left(-Cos(\tfrac{\xi}{2})|0\rangle + e^{\iota\phi}Sin(\tfrac{\xi}{2})|1\rangle\right) + |\Phi_{12}^{-}\rangle\left(Cos(\tfrac{\xi}{2})|1\rangle + e^{\iota\phi}Sin(\tfrac{\xi}{2})|0\rangle\right) + |\Phi_{12}^{+}\rangle\left(Cos(\tfrac{\xi}{2})|1\rangle - e^{\iota\phi}Sin(\tfrac{\xi}{2})|0\rangle\right)\Big] \tag{1.52}$$

Eq. (1.52) clearly shows four equally likely measurement outcomes for Alice, i.e., $|\Psi^{-}\rangle$ or $|\Psi^{+}\rangle$ or $|\Phi^{-}\rangle$ or $|\Phi^{+}\rangle$ with a probability of $\frac{1}{4}$. For example, if Alice's measurement outcome is $|\Psi^{-}\rangle$ then the state of Bob's qubit is superimposed to the teleported state up to an arbitrary phase factor, and therefore Bob retrieves the teleported state without the need to perform a unitary transformation, subject to Alice informing him about her measurement outcome. Clearly without Alice informing Bob regarding her measurement outcomes, Bob will never be able to retrieve the original information- at the best he can only guess the measurement outcome with a probability of $\frac{1}{4}$ which further decreases for the case of a multi-qubit information transfer. In fact, Bob has no way to interpret the state of his qubit even if he tries to do so without the two-bit classical information received from Alice. This very fact prevents quantum teleportation to communicate faster than light. Similarly, if Alice's measurement outcomes are $|\Psi^{+}\rangle$, $|\Phi^{-}\rangle$ or $|\Phi^{+}\rangle$, then Bob needs to perform σ_z, σ_x, σ_y operations, respectively on his qubit to recover the original information. Nevertheless, in all the four cases, Bob gets the teleported state and the protocol is realized successfully. Further, the protocol does not violate the No-Cloning theorem as the original state gets destroyed in the process of teleportation, thus no question of having two copies of the same state. Interestingly, the protocol can be used to create a network for teleporting the state from one participant to another or for a two way teleportation where Bob may use the teleported state as the input state to communicate back to the sender or to communicate it further to another user in the protocol. Due to the way protocol is defined, teleportation can be highly beneficial to establish secure communication between different users.

An obvious question that one may ask is about reliability of the protocol or the efficiency of the quantum channel used to implement the protocol. Therefore, as a criterion for successful teleportation, one can compute teleportation fidelity which indicates the degree of overlap between input and output states. For example, fidelity of quantum teleportation can be expressed as the overlap of input state $|\psi_{in}\rangle$ and output state ρ_{out} as

$$F = \langle\psi_{in}|\rho_{out}|\psi_{in}\rangle \tag{1.53}$$

Since the initial state is unknown, the average fidelity [Massar and Popescu, 1995] can also be given as,

$$F_{avg} = \frac{1}{4\pi}\int_0^{2\pi} d\phi \int_0^{\pi} F Sin(\xi) d\xi \tag{1.54}$$

As the quantum state is teleported without the requirement of any medium, the information content is completely secure once the entangled qubits are distributed securely over a quantum channel. Considering the importance of protocol, a lot of theoretical and experimental progress have been made towards realizing the teleportation of arbitrary states [Horodecki *et al.*, 1996; Bouwmeester *et al.*, 1997; Boschi *et al.*, 1998; Karlsson and Bourennane, 1998; Jennewein *et al.*, 2001; Ursin *et al.*, 2004; Riebe *et al.*, 2004a; Agrawal and Pati, 2006; Ursin *et al.*, 2007; Jung *et al.*, 2008; Kumar and Krishnan, 2009b; Man and Xia, 2012; Takesue *et al.*, 2015; Ren *et al.*, 2017; Basset *et al.*, 2021].

On the experimental front, the original protocol proposed by C. H. Bennett *et al.* [Bennett *et al.*, 1993] was first implemented using photonic qubits by Bouwmeester *et al.* [Bouwmeester *et al.*,

1997] in 1997 and Boschi *et al.* [Boschi *et al.*, 1998] in 1998. Following this, different variants of quantum teleportation were proposed using Nuclear Magnetic Resonance (NMR) [Nielsen *et al.*, 1998], optical modes [Zhang *et al.*, 2003; Lee *et al.*, 2011b], atomic ensembles [Bao *et al.*, 2012; Krauter *et al.*, 2013], trapped atoms [Riebe *et al.*, 2004b, 2007; Nölleke *et al.*, 2013] and solid state systems [Gao *et al.*, 2013; Pfaff *et al.*, 2014]. The academic community has already witnessed great advances in terms of teleporting a quantum state over arbitrary distances. For example, in August 2004, Ursin *et al.* [Ursin *et al.*, 2004] demonstrated a high-fidelity teleportation experiment of photons over a distance of 600 meters across the river Danube in Vienna. Further, as shown in Refs. [Jin *et al.*, 2010b; Ma *et al.*, 2012], the record distance for quantum teleportation was progressively increased to 16 kms in 2010, and 143 kms in 2012 between two of the Canary Islands of La Palma and Tenerife. Similarly, in 2016, Raju Valivarthi *et al.* [Valivarthi *et al.*, 2016] teleported the quantum state of a photon over 6 kilometers under the city of Calgary, i.e., in the actual city infrastructure- this was considered as a new record for quantum teleportation over arbitrary distances, that too in an actual metropolitan network. In 2017, the team led by J.W. Pan [Ren *et al.*, 2017] teleported independent single-photon qubits over distances of up to 1,400 kilometers from a ground observatory at Ngari to a low-Earth-orbit satellite-Micius, which is the current record for the farthest quantum teleportation. The inherent properties of teleportation protocol further allow its applications in entanglement swapping [Pan *et al.*, 1998; Jennewein *et al.*, 2001], quantum repeaters [Briegel *et al.*, 1998; Dias and Ralph, 2017], quantum computation [Brassard *et al.*, 1998; Deutsch and Ekert, 1998; Gottesman and Chuang, 1999; Gao *et al.*, 2010] and quantum internet [Kimble, 2008; Wehner *et al.*, 2018; Cacciapuoti *et al.*, 2020].

1.4.2 Controlled teleportation

Interestingly, for an entangled resource with three or more than three qubits, there is a possibility of introduction of a controller (or controllers) in the protocol who can control the information content between the sender and the receiver. The teleportation protocol with the involvement of a controller is known as controlled teleportation protocol [Karlsson and Bourennane, 1998]. In the simplest case of three participants, the protocol advocates transmission of information by a sender to any one of the participants, but not to the both. This is obvious as the No-Cloning theorem prevents the creation of additional copies of the input state. However, at a particular stage of the protocol, participants other than the sender share the unknown information as part of an entangled state shared between the two. At this stage, the sender may ask one of the other two participants to act as a controller and assist the receiver to successfully retrieve the unknown information. Of course the controller, depending on his measurement basis, can control the information content between the sender and the receiver. For a maximally entangled shared resource between a sender, a controller and a receiver, an appropriate choice of the measurement basis by the controller always leads to the successful teleportation with unit fidelity.

Here, we proceed to provide a brief review of the controlled teleportation protocol using a three-qubit shared entangled resource between the participants. In the original protocol Alice wants to send an unknown quantum state $|\psi_{in}\rangle_1 = Cos\frac{\xi}{2}|0\rangle_1 + e^{\iota\phi}Sin\frac{\xi}{2}|1\rangle_1$ either to Bob or Cliff using a three-qubit maximally entangled Greenberger-Horne-Zeilinger (GHZ) state $|\Psi^-_{ABC}\rangle = \frac{1}{\sqrt{2}}[|000\rangle + |111\rangle]_{ABC}$ where the subscripts denote the distribution of particles to the three participants. As the shared resource is completely symmetrical with respect to the permutation of qubits, Alice, Bob and Cliff can assume any of the qubits from the shared resource. For convenience, we consider qubit A to be with Alice, qubit B to be with Bob and qubit C to be with Cliff. In order to teleport the unknown state, Alice performs a Bell State measurement (BSM) on the joint state of her qubits comprising the unknown qubit and her qubit A in the shared entangled resource. Similar to the Eq. (1.52), BSM projects the joint state of Bob's and Charlie's qubit onto one of the four possible two-qubit entangled states depending on Alice's measurement outcomes

such that

$$|\psi_{1ABC}\rangle = \frac{1}{2}\Big[|\Psi^-_{1A}\rangle \left(Cos(\tfrac{\xi}{2})|01\rangle - e^{\iota\phi}Sin(\tfrac{\xi}{2})|10\rangle\right)_{BC} + |\Psi^+_{1A}\rangle \left(Cos(\tfrac{\xi}{2})|01\rangle + e^{\iota\phi}Sin(\tfrac{\xi}{2})|10\rangle\right)_{BC}$$
$$+ |\Phi^-_{1A}\rangle \left(Cos(\tfrac{\xi}{2})|00\rangle - e^{\iota\phi}Sin(\tfrac{\xi}{2})|11\rangle\right)_{BC} + |\Phi^+_{1A}\rangle \left(Cos(\tfrac{\xi}{2})|00\rangle + e^{\iota\phi}Sin(\tfrac{\xi}{2})|11\rangle\right)_{BC}\Big] \quad (1.55)$$

Here, we consider one of the cases where Alice's measurement outcome is $|\Phi^+_{1A}\rangle$ such that the joint state of other two qubits is $\left[Cos(\frac{\xi}{2})|00\rangle + e^{\iota\phi}Sin(\frac{\xi}{2})|11\rangle\right]_{BC}$. All the four cases, however, are equivalent to each other and can be treated in a similar fashion. If Alice wants to communicate the unknown state to Bob (Cliff), she advises Cliff (Bob) to perform an appropriate single qubit measurement on his qubit. Suppose Cliff acts as a controller and measures his qubit in a general basis represented as

$$\begin{aligned} |u_1\rangle_C &= Cos\theta\,|0\rangle_C + Sin\theta\,|1\rangle_C \\ |u_2\rangle_C &= Sin\theta\,|0\rangle_C - Cos\theta\,|1\rangle_C \end{aligned} \quad (1.56)$$

Clearly, if Cliff measures the state of his qubit in the computational basis, the protocol is unsuccessful, i.e., the receiver will not be able to retrieve the teleported state. However, if Cliff measures the state of his qubit in $|+\rangle$, $|-\rangle$ basis, then the teleportation is deterministic. In all other cases, the average fidelity of teleportation depends on the parameter associated with the measurement basis of the controller, i.e., $F_{avg} = \frac{2}{3} + \frac{1}{3}Sin2\theta$. For $\theta = \frac{\pi}{4}$, the average fidelity is unity indicating the perfect teleportation. However, if $\theta = 0$ then the average fidelity is $\frac{2}{3}$- equivalent to the classical case.

Recently a different perspective of controlled teleportation is discussed from the point of view of the controller [Li and Ghose, 2014, 2015]. For controlled teleportation, the authority of controller is essential and without the help of the controller, fidelity [Massar and Popescu, 1995] should not exceed the classical limit of $\frac{2}{3}$. Considering that the perfect teleportation with optimal measurement of the controller leads to unit fidelity, the lower bound for the controller's power is $\frac{1}{3}$. Therefore, protocols where controller's power is less than the lower bound render the controller powerless, and hence the shared resources in such cases are not suitable for controlled teleportation from a controller's perspective. A controlled protocol with multiple controllers also has interesting applications in multiparty entanglement swapping and multiuser cryptographic networks [Biham *et al.*, 1996; Townsend, 1997; Bose *et al.*, 1998; Hamdoun and Sagheer, 2020; Zhang and Li, 2021].

1.4.3 Quantum dense coding

In 1992, Bennett and Wiesner [Bennett and Wiesner, 1992] demonstrated one of the simplest applications of quantum entanglement for efficiently communicating classical information between two users in a protocol- *quantum dense coding*. Classically, one can communicate one-bit information by locally manipulating and sending the single bit to the another user in the protocol. However, if a sender and a receiver share a maximally entangled state of two qubits, then the sender can send two bits of classical message by manipulating her/his share of qubit in the shared entangled state. If the operations performed by the sender are restricted to Pauli operators and identity operator, then the dense coding protocol is also termed as super dense coding protocol. In the simplest case, the sender can prepare four different orthogonal set of maximally entangled states by locally manipulating the shared entangled state. By performing single qubit unitary operations, the sender maps the shared Bell state to any of the four Bell states. For example, if the shared entangled state is $|\Phi^+_{SR}\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]_{SR}$ where the qubit indices S and R stand for the sender and the receiver then the sender can locally manipulate her/his qubit S by performing unitary operations such as I, σ_x, σ_{iy} and σ_z depending on the need of information to be transferred. These operations clearly enable the sender to map the shared entangled state into one of the Bell

states, i.e., $|\Phi^+_{SR}\rangle$ or $|\Psi^+_{SR}\rangle$ or $|\Psi^+_{SR}\rangle$ or $|\Psi^-_{SR}\rangle$. Once the sender encodes the information, she/he sends the qubit to the receiver who in turn performs a joint two-qubit Bell-state measurement to decode the message, based on a prior agreement on the encoding scheme. Therefore, using the protocol the sender is able to communicate two bits of classical message using a single qubit. Similarly, if the sender and the receiver share a $2N$-qubit entangled state then the sender can perform 4^N operations on her/his N qubits to map the original state to 2^{2N} distinct orthogonal states. The receiver can, in principle, distinguish the encoded orthogonal states to decrypt the message. Hence, use of N pairs of maximally entangled states results in the transmission of $2N$ bits of information, thereby doubling the classical information capacity of a channel.

The dense coding capacity [Bowen, 2001] for a quantum system ρ_{AB} can be used as a measure of its efficiency to transmit classical information, and is given by

$$C = log_2(D_A) + S(\rho_B) - S(\rho_{AB}) \tag{1.57}$$

where D_A is the dimension of Alice's sub-system, $S(\rho)_B$ is von-Neumann entropy of Bob's sub-system, and $S(\rho)_{AB}$ is von-Neumann entropy of the original shared pure entangled state. Here, qubit A is with Alice (sender) and qubit B is with Bob (receiver). For a maximally entangled two-qubit pure state, $D_A = 2$, $S(\rho)_B = 1$ and $S(\rho)_{AB} = 0$; therefore Eq. (1.57) leads to $C = 2$.

The dense coding protocol was put on the experimental forefront by Mattle *et al.* [Mattle *et al.*, 1996] in 1997 using photon-entangled pairs generated through parametric down-conversion. Subsequently, the experimental demonstration was extended using techniques of Nuclear Magnetic Resonance (NMR) [Fang *et al.*, 2000; Zhang *et al.*, 2005], and using partially entangled and mixed states [Bose *et al.*, 2000]. For multi-qubit resources, the protocol can be established between two or more than two users for communicating classical information [Greenberger *et al.*, 1989; Mermin, 1990a; Dür *et al.*, 2000; Higuchi and Sudbery, 2000; Briegel and Raussendorf, 2001; Acin *et al.*, 2001; Brown *et al.*, 2005; Gour and Wallach, 2010; Zhang and He, 2014; Wei *et al.*, 2018b; Kolusu and Anand, 2021]. The multiqubit case further offers the possibility of controlled dense coding where a controller or many controllers can control the information transfer between a sender and a receiver [Hao *et al.*, 2001; Huang *et al.*, 2009; Jiang *et al.*, 2009; Yi *et al.*, 2011; Nie *et al.*, 2013; Roy and Ghosh, 2015; Liu *et al.*, 2016; Wei *et al.*, 2018b; Ma *et al.*, 2021]. In the simplest case of a shared three-qubit GHZ state, the average information transfer between the sender and the receiver is $1 + 2Sin^2\theta$ where θ represents the parameter associated with the measurement basis of the controller as in Eq. (1.56). In the last three decades, a substantial amount of progress has been made in demonstrating and studying variants of dense coding protocol both on theoretical as well as experimental fronts [Bose *et al.*, 2000; Bruß *et al.*, 2004; Li *et al.*, 2002; Jing *et al.*, 2003; Schaetz *et al.*, 2004; Barreiro *et al.*, 2008; Liu *et al.*, 2013; Guo *et al.*, 2019; Gupta *et al.*, 2021; Moreno *et al.*, 2021].

Originally, the idea of superdense coding was restricted to performing four single-qubit unitary operations (Pauli gates) and transferring two bits of information, however, Westfall [Westfall, 2020] proposed a scheme named '*SuperDense Coding Beyond the Pauli Gates*', to encode a fifth state in the superdense coding protocol, making it possible to communicate more than four states, i.e., two bits of information. Recently, superdense coding has also been used for quantum signature [Lou *et al.*, 2019; Niu *et al.*, 2020], which has a wide application in e-payment [Xiaojun, 2010; He *et al.*, 2021], e-voting [Bonanome *et al.*, 2011], e-commerce [Thapliyal and Pathak, 2019], e-health [Perumal and Nadar, 2020] etc.

1.5 BACKGROUND AND MOTIVATION

1.5.1 The Bell inequality

One of the most intriguing features of quantum theory is the existence of non-local correlations that are fundamentally different from classical correlations. This difference becomes

more evident with the violation of Bell or Bell-type inequalities by states exhibiting quantum correlations between qubits [Bell, 1964]. Clearly states violating the Bell-type inequalities confirm the presence of genuine non-local correlations between qubits. Recent advances, however, show that nonlocality is not confined to violation of Bell-type inequalities only, i.e., there are states which are entangled or possess nonlocal correlations for a range of the state parameter but may still not violate Bell inequalities. In view of the above, in the present section, we will shed light into the complex nature of entanglement and nonlocality in bi-partite mixed and multiqubit states.

In one of its simplest form, the Bell inequality can be defined using Clauser, Horne, Shimony, and Holt (CHSH) inequality, also known as the Bell-CHSH inequality [Clauser *et al.*, 1969] where the Bell-CHSH operator for a two-qubit system can be defined as

$$B_{CHSH} = \langle AB \rangle + \langle AB' \rangle + \langle A'B \rangle - \langle A'B' \rangle \tag{1.58}$$

For a general two-qubit state, $A = \vec{a}.\vec{\sigma}_1$ and $A' = \vec{a'}.\vec{\sigma}_1$ represent measurements performed on the first subsystem. Similarly $B = \vec{b}.\vec{\sigma}_2$ and $B' = \vec{b'}.\vec{\sigma}_2$ represent measurements performed on the second subsystem. Here $\vec{\sigma}_i = \{\sigma_x, \sigma_y, \sigma_z\}$ (with $i = 1, 2$) are Pauli operators associated with respective qubits and $\vec{a}, \vec{a'}, \vec{b}, \vec{b'}$ are unit vectors in $\mathbb{R}^3$, defined as

$$\begin{aligned}
\vec{a} &= (Sin\theta_a Cos\phi_a, Sin\theta_a Sin\phi_a, Cos\theta_a) \\
\vec{a'} &= (Sin\theta_{a'} Cos\phi_{a'}, Sin\theta_{a'} Sin\phi_{a'}, Cos\theta_{a'}) \\
\vec{b} &= (Sin\theta_b Cos\phi_b, Sin\theta_b Sin\phi_b, Cos\theta_b) \\
\vec{b'} &= (Sin\theta_{b'} Cos\phi_{b'}, Sin\theta_{b'} Sin\phi_{b'}, Cos\theta_{b'})
\end{aligned} \tag{1.59}$$

As discussed previously, the Bell-CHSH inequality- based on the assumptions of locality and realism- is bounded by $|\langle B_{CHSH} \rangle_\rho| \leq 2$, where ρ refers to a two-qubit pure or mixed quantum state. It is evident that for a two-qubit pure entangled state, the violation of inequality increases with the increase in degree of bipartite entanglement [Gisin, 1991; Popescu and Rohrlich, 1992]. Although all two-qubit pure entangled states violate the Bell-CHSH inequality, interestingly the inequality is not violated by all two-qubit mixed entangled states for the complete range of state parameters [Werner, 1989; Horedecki *et al.*, 1996; Aravind, 1995; Peres, 1996a; Munro *et al.*, 2001a; Gisin, 1996a]. For example, as shown in Figure 1.4, the Werner state [Werner, 1989] given by

$$\rho_w = \frac{1-a}{4} I + a \left|\psi^-\right\rangle \left\langle\psi^-\right|, \tag{1.60}$$

though entangled for $a > \frac{1}{3}$, violates the Bell-CHSH inequality only for the range $\frac{1}{\sqrt{2}} < a \leq 1$ where a represents the state parameter, $|\psi^-\rangle$ represents the two-qubit maximally entangled anti-symmetric singlet state and I represents the white noise [Vértesi, 2008]. Therefore, the Bell-CHSH inequality fails to detect nonlocal correlations in a Werner state for the range $\frac{1}{3} < a \leq \frac{1}{\sqrt{2}}$. On the other hand, quantum discord [Ollivier and Zurek, 2001] which is a measure of nonlocal correlation, and captures the nonlocality in entangled as well as separable bipartite systems, confirms that the state exhibits nonlocal correlations over the complete range of the state parameter a [Luo, 2008; Dakić *et al.*, 2010; Singh and Kumar, 2018c]. Similar observations can be made for other bipartite mixed entangled states such as Horodecki states and maximally entangled mixed states (MEMS) [Horedecki *et al.*, 1996; Munro *et al.*, 2001b]. To be precise, Horodecki states represented as,

$$\rho_H = b \left|\Phi^+\right\rangle \left\langle\Phi^+\right| + (1-b) \left|00\right\rangle \left\langle 00\right| \tag{1.61}$$

and MEMS states represented as,

$$\rho_{MEMS} = \begin{bmatrix} g(\gamma) & 0 & 0 & \gamma/2 \\ 0 & 1-2g(\gamma) & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \gamma/2 & 0 & 0 & g(\gamma) \end{bmatrix} \text{ where } g(\gamma) = \begin{cases} 1/3, & \gamma < \frac{2}{3} \\ \gamma/2, & \gamma \geq \frac{2}{3} \end{cases} \tag{1.62}$$

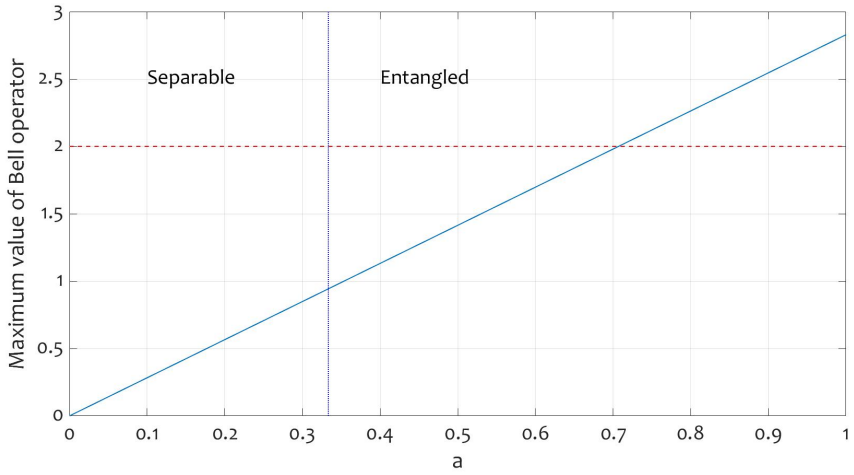

Figure 1.4 : Violation of the Bell inequality by Werner states

are entangled for the complete range of respective state parameters b and γ, but fails to violate the Bell-CHSH inequality in the range $0 < b \leq \frac{1}{\sqrt{2}}$ and $0 < \gamma \leq \frac{1}{\sqrt{2}}$, respectively where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The properties of these set of states have extensively studied not only to understand the fundamental aspects of quantum information and computation, but also for their use as resources in quantum information processing. Therefore, there is a need to further study correlations from a perspective different than the entanglement versus separability paradigm.

1.5.2 Bell-type inequalities for multiqubit states

As discussed in previous sections, multiqubit entanglement and nonlocality is a much more complex problem to execute in comparison to bi-partite systems. The difficulty level and complexity increases enormously with the increase in number of qubits in an underlying state. For example, three qubit pure states can be classified into two inequivalent classes whereas four qubit pure states require nine different classes for complete classification [Verstraete *et al.*, 2002]. Moreover, simple generalization of entanglement and nonlocality measures from bipartite system to multiqubit systems is not possible. Although quantum discord describes nonlocal correlations in all bipartite system, it is difficult to obtain analytical expressions to evaluate discord pertaining to the optimization procedure involved. Similarly, for three qubit states, one may evaluate dissension [Chakrabarty *et al.*, 2011] to measure the quantumness of correlations but the measure again suffers from the similar optimization procedure involved. In this subsection, we discuss some key features of multiqubit nonlocality.

For three-qubit entangled systems, nonlocality between qubits can be characterized using the Mermin inequality [Mermin, 1990b; Chi *et al.*, 2010], namely

$$|M| = \langle ABC\rangle - \langle AB'C'\rangle - \langle A'BC'\rangle - \langle A'B'C\rangle \leq 2 \tag{1.63}$$

where $A(A')$, $B(B')$ and $C(C')$ are measurements performed on the first, second and third subsystems, respectively. Unfortunately, the above inequality fails to distinguish between bipartite and genuine tripartite correlations as the inequality is violated by bi-separable as well as genuinely entangled three qubit states. Moreover, within the set of three-qubit pure generalized Greenberger-Horne-Zeilinger (GGHZ) states $|\psi_{GGHZ}\rangle = Cos(\theta)|000\rangle + e^{i\phi}Sin(\theta)|111\rangle$, the inequality also fails to characterize nonlocality in a large set of states. For example, the Mermin inequality is violated by GGHZ states only for $\theta > \frac{\pi}{12}$ (Figure 1.5).

However for three-qubit systems, the Svetlichny inequality [Svetlichny, 1987] distinctly differentiates between bi-partite and tripartite nonlocality and acts as a signature for genuine

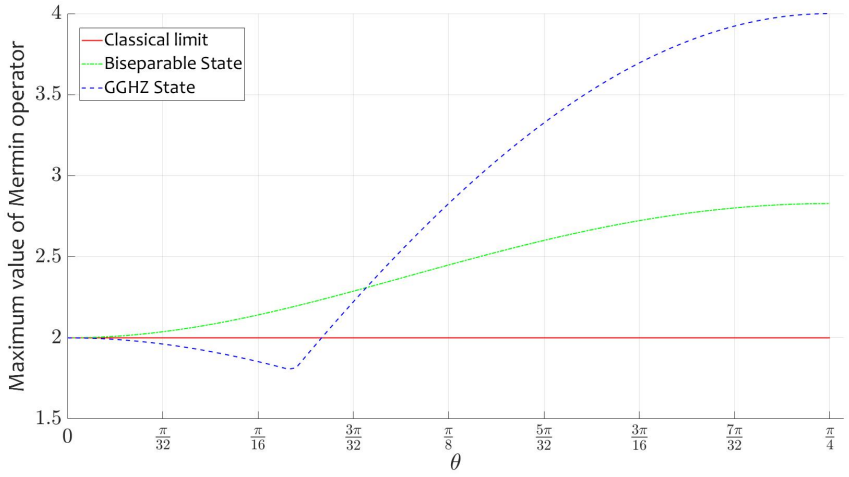

Figure 1.5 : Violation of the Mermin inequality

tripartite nonlocality. The three-qubit Svetlichny inequality is represented as

$$|S| = \langle ABC\rangle + \langle AB'C\rangle + \langle ABC'\rangle - \langle AB'C'\rangle + \langle A'BC\rangle - \langle A'B'C\rangle - \langle A'BC'\rangle - \langle A'B'C'\rangle \leq 4 \tag{1.64}$$

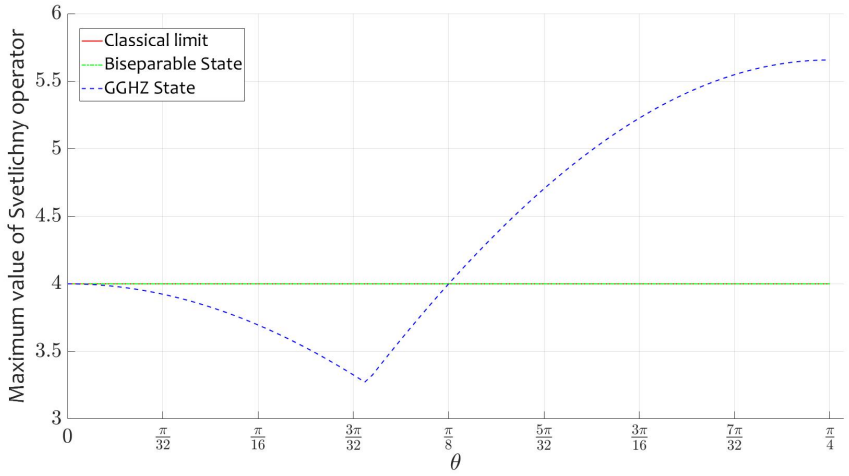

Figure 1.6 : Violation of the Svetlichny inequality

Although the violation of Svetlichny inequality confirms the presence of genuine three-qubit correlations only, the inequality fails to characterize nonlocal correlations in GGHZ states for $\theta \leq \frac{\pi}{8}$. Figure 1.6 clearly demonstrates that the Svetlichny inequality bears a stamp of genuine tripartite correlation as against bipartite correlations in a bi-separable state. Interestingly, for three-qubit systems, no generic inequality is found to identify nonlocal correlations in all entangled states. In general, for multiqubit systems, the problems of classifying and quantifying nonlocal correlations- by designing an inequality to characterize nonlocality- is highly complex and interesting due to the intricacies involved. Clearly, the situation becomes even more challenging if one includes analysis of multiqubit mixed states as well. In fact, the case of multiqubit pure states for distinction and characterization of genuine nonlocal correlations itself requires a much better physical interpretation.

Similar to the Bell-CHSH inequality [Bell, 1964; Clauser *et al.*, 1969] which efficiently captures nonlocal correlations in two-qubit entangled states, Gisin and Bechmann [Gisin and Bechmann-Pasquinucci, 1998] demonstrated a logical generalization of the Bell-CHSH inequalities

for the case of n-qubits to characterize maximally entangled states of n-qubits. The generalization was initially proposed by Klyshko and Belinskii [Belinskiĭ and Klyshko, 1993]- the maximal violation of the generalized inequality was found to be larger than the inequalities independently proposed by Mermin and Ardehali [Mermin, 1990a; Ardehali, 1992; Belinskiĭ and Klyshko, 1993]. This generalization is referred in literature as MABK [Żukowski *et al.*, 2002], MBK [Acin *et al.*, 2002b] or MK [Scarani and Gisin, 2001] and can be expressed as

$$M_n = \frac{1}{2}M_{n-1}(a_n + a'_n) + \frac{1}{2}M'_{n-1}(a_n - a'_n) \tag{1.65}$$

where $a_n = \pm 1$ and $a'_n = \pm 1$ denote the only possible outcomes of two available measurements to be performed on the nth qubit. Further, M'_n can be defined in a similar manner as M_n with all the primed and non-primed a's exchanged. The generalized inequality resembles the two-qubit Bell inequality and in fact reduces to the Bell-CHSH inequality (Eq. (1.58)) for $n = 2$. Similar to the maximum violation of Bell-CHSH inequality by two-qubit maximally entangled Bell states, the n-qubit inequality is maximally violated by the maximally entangled n-qubit *GHZ* state [Gisin and Bechmann-Pasquinucci, 1998]. Interestingly, the generalized inequality discussed above further reduces to the Mermin inequality for $n = 3$ as represented in Eq. (1.63). As described earlier, the other efficient classification of three-qubit inequality is the Svetlichny inequality which is proved to be better than the Mermin inequality in terms of distinguishing bi-partite correlations from genuine tripartite correlations. Clearly, the three-qubit Svetlichny inequality (Eq. (1.64)) can not be directly obtained from the above discussed n-qubit generalization of the Bell-CHSH inequalities. Considering the importance of Svetlichny inequality, Collins *et al.* [Collins *et al.*, 2002] proposed generalized Svetlichny polynomial S_n using M_n of Eq. (1.65) as

$$S_n = \begin{cases} M_n, & n \text{ even} \\ \frac{1}{2}\left(M_n + M'_n\right), & n \text{ odd.} \end{cases} \tag{1.66}$$

Both the generalized inequalities represented in Eq. (1.65) and Eq. (1.66) are maximally violated by maximally entangled n-qubit GHZ states. For example, if we consider three-qubit systems, then Mermin (Eq. (1.63)) and Svetlichny (Eq. (1.64)) inequalities are maximally violated by the three-qubit maximally entangled GHZ state. Moving forward to four-qubit systems, the MABK or Svetlichny [Seevinck and Svetlichny, 2002] inequality is expressed as

$$\begin{aligned} &E_{1111} - E_{1112} - E_{1121} - E_{1211} - E_{2111} - E_{1122} - E_{1212} - E_{2112} - E_{1221} - E_{2121} - E_{2211} \\ &\quad + E_{2221} + E_{2212} + E_{2122} + E_{1222} + E_{2222} \leq 4 \end{aligned} \tag{1.67}$$

where E_{ijkl} represents the expectation value $E(A_iB_jC_kD_l)$. The four qubit MABK or Svetlichny inequality is also maximally violated by the four-qubit maximally entangled GHZ state. The other important classes of entangled states for four qubits are cluster [Briegel and Raussendorf, 2001] and $|\chi\rangle$ states [Yeo and Chua, 2006] which are extensively used in literature for efficient applications in quantum information and computation [Yeo and Chua, 2006; Wu *et al.*, 2007; Lin *et al.*, 2008; Gao, 2010; Qu *et al.*, 2011; Xiu *et al.*, 2011; Liu *et al.*, 2012b; Yin *et al.*, 2012; Luo and Deng, 2013; Dong *et al.*, 2013; Yang *et al.*, 2018; Lv and Zhou, 2020]. Considering the importance of cluster states [Briegel and Raussendorf, 2001] for one-way quantum computer [Raussendorf and Briegel, 2001], Scarani *et al.* proposed a four-qubit inequality [Scarani *et al.*, 2005] specially designed for cluster states- later named SASA inequality- and represented as

$$E(A_2B_1C_1D_1) + E(A_1C_1D_2) + E(A_1C_2D_1) - E(A_2B_1C_2D_2) \leq 2 \tag{1.68}$$

Evidently, the SASA inequality is optimally violated by cluster states [Wu *et al.*, 2007] but the same inequality is not violated by the maximally entangled four-qubit GHZ state. In order to describe

nonlocality in $|\chi\rangle$ states, Wu *et al.* [Wu *et al.*, 2007] proposed another four-qubit Bell-type inequality given by

$$E(A_1B_1C_1D_1)+E(B_1C_2D_2)+E(B_2C_1D_2)-E(A_1B_2C_2D_1)\leq 2 \tag{1.69}$$

The $|\chi\rangle$ states are shown to be efficient resources for perfect teleportation of an arbitrary two-qubit state [Yeo and Chua, 2006]. Since the inequality was designed specifically for the $|\chi\rangle$ state, it is optimally violated by $|\chi\rangle$ states. However, this inequality is not violated by the GHZ class and is non-optimally violated by linear cluster states. $|\chi\rangle$ states also violate MABK and SASA inequalities with the extent of violation being non-optimal. Although these inequalities can definitely be used to classify correlations in specific classes of states, they also suffer from indistinguishability between genuine four-qubit versus three-qubit nonlocality. Clearly, these inequalities are also violated by bi-separable states where one of the partitions is a three-qubit GHZ state, and tri-separable states where one of the partitions is a Bell state. In addition, the MABK inequality even shows violation for another type of bi-separable state where both the partitions are represented by Bell states. Therefore, these inequalities fail to effectively distinguish between two-, three- and four-qubit nonlocal correlations even within the entangled classes of pure four-qubit systems. Hence, the design of a generic inequality to identify genuine four-qubit nonlocality will therefore be of immense value.

1.5.3 Applications of partially entangled states

In order to optimize the efficiency of a particular protocol or a task for a noiseless channel, a maximally entangled state is considered as an ideal resource [Ekert, 1991; Bennett *et al.*, 1993; Hillery *et al.*, 1999; Bennett and Wiesner, 1992; Karlsson and Bourennane, 1998]. However, if the shared entangled resource between the users is a non-maximally or a partially entangled state then the efficiency of the protocol decreases significantly owing to the different properties of nonlocal correlations in non-maximally/partially entangled states as against the maximally entangled states [Popescu, 1994; Mor, 1996; Mor and Horodecki, 1999; Horodecki *et al.*, 1999; Banaszek, 2000; Li *et al.*, 2000; Kurucz *et al.*, 2001; Gour, 2004]. For example, if a three-qubit partially entangled general W state is used as a resource for teleportation then the fidelity of the protocol depends on coefficients associated with the unknown state to be teleported [Shi and Tomita, 2002]. Moreover, the protocol is probabilistic in nature and maximum probability for the successful teleportation in this case is $\frac{2}{3}$ for a standard W state. Similarly, for a dense coding protocol, using the maximally entangled three-qubit GHZ state, Alice can communicate 3 bits of information to Bob by locally manipulating her two qubits. Whereas, if a partially entangled GHZ state, i.e., $\cos\theta\,|000\rangle+\sin\theta\,|111\rangle$ is used as a resource, then Alice can only communicate $(1+\sin^2 2\theta)$ of information to Bob by locally manipulating her two qubits where $0<\theta\leq\frac{\pi}{4}$. The partially entangled W class of states are not efficient resources for superdense coding protocol. Agrawal and Pati [Agrawal and Pati, 2002; Pati and Agrawal, 2004] proposed a generalized but probabilistic quantum teleportation protocol using a non-maximally entangled state as a quantum resource. They further extended the study to describe a generalized protocol for entanglement swapping using non-maximally entangled states.

Interestingly, Pati and Agrawal [Agrawal and Pati, 2006] also proposed a set of partially entangled W_n states for successful teleportation of a single qubit by performing joint measurements in the same basis. They demonstrated perfect teleportation protocol with unit fidelity subject to the experimental realization of the proposed set of states, and successfully distinguishing the set of three-qubit partially entangled states in an experiment. These set of states are also shown to be efficient in superdense coding protocol such that Alice can communicate 2-bit of information to Bob by locally manipulating her single qubit. Within the class of three-qubit entangled systems, W and W_n states are extensively used in literature for realizing several quantum information processing tasks [Cao and Song, 2005; Li and Qiu, 2007; Chen *et al.*, 2008; Li *et al.*, 2008, 2009; An, 2010; Nie

et al., 2011c; Hwang *et al.*, 2011; Nie *et al.*, 2011a]. This was further followed by characterizing entanglement, nonlocality and efficiency of partially entangled states for quantum information and computation [Barenco and Ekert, 1995; Eisert and Plenio, 1999; Lee and Kim, 2000; Kurucz *et al.*, 2001; Gour, 2004; Pati *et al.*, 2005; Yang *et al.*, 2009b; Rigolin, 2009; Wang and Yan, 2009; Chimczak and Tanaś, 2009; Gordon and Rigolin, 2010; Pathak and Banerjee, 2011; Sheikhehi and Naseri, 2011; Bandyopadhyay and Ghosh, 2012; Fortes and Rigolin, 2013; Liang *et al.*, 2013; Ai *et al.*, 2014; Cai *et al.*, 2014; Li and Ghose, 2014; Wang *et al.*, 2014a; Wang and Shu, 2015; Wang *et al.*, 2015; Xiong *et al.*, 2016; Wei *et al.*, 2018a; Singh and Kumar, 2018a; Faujdar and Kumar, 2019; Kaur and Kumar, 2019; Ishizaka, 2020; Faujdar and Kumar, 2021; Javed *et al.*, 2021]. The usefulness and efficiency of partially entangled states for quantum information and computation has led either to several successful experimental realization of such states or proposals for implementing an experiment to realize partially entangled states [Azuma, 2000; Yamamoto *et al.*, 2001; Thew *et al.*, 2002; He *et al.*, 2013; Cao *et al.*, 2016; Zhang *et al.*, 2018, 2019b; Gómez *et al.*, 2019; Zhang *et al.*, 2019a, 2020; Bian *et al.*, 2020; Tyagi and Wharton, 2022].

The use of partially entangled states for quantum information processing becomes much more pronounced in noisy conditions. In a noisy environment, the input entangled pure state evolves into a mixed state under the influence of a noisy channel. The efficiency of the protocol therefore depends on the input state, its properties and how the nonlocal correlations evolve under the influence of the noisy channel. The mechanism to protect nonlocal correlations further influences the optimal efficiency of the protocol depending on the input pure state, and parameters involved in the protocol. One of the interesting problems would be to address the efficiencies of partially entangled multiqubit states and then compare it with corresponding maximally entangled states in different scenarios. The study will definitely lead to useful resources in real noisy conditions. It will be beneficial for actual experimental set-up to take informed decisions with respect to the use of the input entangled resources for a particular protocol.

1.6 RESEARCH OBJECTIVES OF THE THESIS

Due to their fundamental importance to theory and applicability to quantum computation, quantum correlations have been the topic of intense debate ever since the inception of quantum theory to describe the less intuitive nature of atomic particles. The analysis of nonlocal correlations in many-body systems allows one to characterize properties of large-scale quantum systems to understand and study the complex and subtle nature of entanglement and nonlocality. Such studies further allow us to analyze and design multi-network protocols for information processing in an optimal manner by establishing relations between the efficiency of a protocol and existing nonlocal correlations and entanglement of the input state. In previous sections, we have discussed the characterization and applications of nonlocal correlations in quantum information and computation. The analysis of Bell and Bell-type inequalities is of paramount interest and therefore in last three decades the academic community has witnessed characterization and generalization of nonlocal correlations in bi-partite and multiqubit pure and mixed states. As discussed in the previous section, most of the multiqubit inequalities fail to distinguish between genuine multi-partite nonlocality versus nonlocality arising due to entanglement between product states comprising lesser number of particles. In fact, the inequalities further fail to identify nonlocal correlations in a larger set of genuinely entangled multiqubit states as well. In certain cases, a particular inequality may be appropriate to characterize a particular class of multiqubit states and hence will be violated by that set of genuinely entangled states but would be satisfied by another set of genuinely entangled multiqubit states. Moreover, in addition to separable states exhibiting nonlocal correlations, there exists mixed entangled states which do not violate the Bell or Bell-type inequalities. Therefore, the need to analyze and characterize nonlocal correlations using a generic approach to understand the properties of multiqubit states and their applications in quantum information. Such studies further facilitate to interpret the relation between nonlocality,

entanglement and efficiency of entangled resources in different protocols under real conditions.

The Thesis aims to readdress the issues of characterization and applicability of nonlocal correlations in quantum information processing. For this, we assess the extent of correlations between qubits using standard Ursell-Mayer type expansion based on the principles of many body statistical mechanics [Fano, 1983; Schlienz and Mahler, 1995; Altafini, 2004; Audenaert and Plenio, 2006; Kumar and Krishnan, 2009a,b]. We further analyze efficiencies of different classes of multiqubit entangled states in light of our analysis of nonlocal correlations in real conditions. The main research objectives of the Thesis are listed below.

- **To develop a useful quantifier of nonlocal correlations for two-qubit pure as well as mixed states**: Although Bell inequalities are violated by all pure two-qubit entangled states, there are sets of mixed states, which do not violate the Bell inequality for a given range of state parameters even if the state is entangled in that region. Moreover, there exist separable states possessing quantum correlations but still satisfying the Bell inequality. Such states are shown to be useful resources for quantum information and computation. As a measure of non-classicality of correlations, quantum discord can be used to identify nonlocal correlations in all two qubit states. However, the involvement of optimization procedure in determination of discord renders its evaluation extremely difficult. Therefore, one of the objectives is to analyze nonlocal correlations in two qubit entangled pure and mixed states. The aim is to perform a detailed analysis to understand non-classicality in entangled as well as separable states. The study further includes analysis in ideal as well as real conditions.

- **To develop useful quantifiers of nonlocal correlations for multiqubit systems**: As discussed above, nonlocal correlations existing between a pair of particles in mixed entangled or separable states itself require substantial attention to understand and establish usefulness of such resources in quantum information processing. Once we increase the number of qubits to address entanglement and nonlocality in states with more than two qubits, the characterization becomes much more involved owing to the increased complexity. For example, multiqubit Bell-type inequalities are not violated by set of pure entangled states until the degree of entanglement exceeds a certain value. This is in contrast to bi-partite states where all pure entangled states violate the Bell inequality. Moreover, the distinguishability between nonlocal correlations arising because of genuine multiqubit entanglement and nonlocal correlations arising due to product of entangled states with fewer number of particles definitely requires to be readdressed. Furthermore, for establishing a multiqubit network with shared entanglement between all participants, one way to ascertain genuine entanglement and nonlocality is that the Bell-type inequality be violated only by genuinely entangled states. Therefore, there is a scope to describe a generic procedure to identify non-classicality of correlations in different classes of multiqubit pure states. Our approach is to study the behavior of nonlocal correlations in pure and mixed multiqubit states using cluster coefficients in ideal and real conditions. The idea is to propose an inclusive procedure to generalize the study of non-classicality in multiqubit pure states and then extend the analysis for different classes of mixed states as well.

- **To analyze efficiencies of partially entangled states for different quantum information processing protocols**: The analysis of quantum correlations is always associated with use of these resources from quantum information and computation. In ideal conditions, a maximally entangled pure state corresponds to the maximal violation of a Bell or Bell-type inequality. However, in real conditions, the input state interacts with the environment and evolves under the influence of noise in such a manner that entanglement of the input state and nonlocality may not coincide and one may find a partially entangled input state to be a better resource in comparison to a maximally entangled input state as far as the efficiency of a particular protocol is concerned. For example, the fidelity of teleportation of a single qubit

as a measure of efficiency of an entangled resource- using a two-qubit or a multiqubit state- may require the user to use a partially entangled state as the input resource depending on the type of noise or the degree of noise. Moreover, even in the ideal conditions, one may have to deal with partially entangled states instead of a maximally entangled state depending on the accuracy of the experiments performed. Therefore, along with the characterization of entanglement and nonlocal correlations, one further needs to perform detailed analysis of efficiency of a protocol using different classes of partially and maximally entangled states in real conditions. The analysis will help one to map out usefulness of these resources to take informed decisions using effective strategies, even before starting an actual experiment. For this purpose, we also aim to analyze efficiencies of partially entangled states for quantum information processing protocols under real conditions in light of the degree of entanglement and existing nonlocal correlations.

1.7 CONTRIBUTIONS OF THE THESIS

To meet the objectives of the Thesis mentioned in the earlier discussion, the following contributions are made.

- **Proposal of an efficient operator to identify nonlocal correlations in two-qubit systems**: In Chapter 2, we readdress the question of analyzing nonlocal correlations in pure and mixed two-qubit entangled states by modifying the existing Bell-CHSH inequality using cluster coefficients- such coefficients indicate the extent of correlations between two qubits and also provide a general definition of bipartite entanglement between qubits. For this, we define a Bell-cumulant inequality, a violation of which confirms the existence of nonlocal correlations in two qubit pure as well as mixed states. Our results further demonstrate nonlocality in pure and mixed two qubit states by establishing an analytical relation between the maximum expectation value of the modified operator and extent of entanglement as measured by concurrence. Interestingly, our results show that the modified operator identifies nonlocal correlations in certain classes of two-qubit mixed states, where the Bell-CHSH operator fails to capture non-classical correlations. In fact, our operator further identifies nonlocal correlations exhibited by separable states, and thus the results are also consistent with discord. We extend our analysis to understand the behavior of nonlocal correlations in noisy conditions with and without applications of weak measurement and its reversal operations to retrieve nonlocal correlations adversely affected due to decoherence. In all the cases discussed in this chapter, analytical results completely agree with the numerical optimization. We further emphasize on usefulness of partially entangled two qubit states and show that the entangled systems where the Bell inequality fails to identify nonlocal correlations are also useful for quantum teleportation.

- **Effective Bell-type operators for multiqubit quantum states**: In general, there is no generic inequality to discuss and compare nonlocality in multiqubit states. In Chapter 3, we readdress the analysis of nonlocal correlations in three qubit pure and mixed states in presence of noise. We start our discussion by establishing an analytical relation between the maximum expectation value of our proposed operator with the three-qubit entanglement measure in the *GGHZ* class and then compare the analytical results with the numerical optimization. For real experimental scenario, we further extend our discussion to characterize nonlocality in three qubit states in presence of noise with and without applications of weak measurement and its reversal operations. For our analysis and comparison of results, we use several sets of pure three-qubit entangled states belonging to *GHZ* and *W* class of states. In order to analyze nonlocal correlations in these states, we propose two different operators based on cluster coefficients and existing Bell-type inequalities. Our results show that the violation of proposed inequalities act as an imprint

of genuine nonlocality between three qubits. Moreover, we further demonstrate that all three-qubit genuinely entangled pure states violate the proposed inequalities for the complete range of three-qubit entanglement measure. Further, our operators also succeed to distinguish between bi-partite and tripartite nonlocality efficiently. Hence, the proposed operators successfully address issues of indistinguishability of different types of nonlocality and issues of sets of genuinely entangled states not violating three-qubit inequalities.

On the similar lines, Chapter 4 demonstrate the suitability of our generic approach to characterize nonlocal correlations in four- and five-qubit entangled classes. Interestingly, our results show that unlike MABK and SASA inequalities, our operators identify nonlocality in all entangled classes. The proposed and modified inequalities are violated by all genuinely entangled pure four and five qubit states, and these inequalities further distinguish genuine nonlocal correlations from bipartite, tripartite or quadripartite nonlocality.

- **Efficiencies of partially entangled states for different quantum information processing protocols**: In order to establish usefulness of different classes of partially and maximally entangled states, Chapter 5 emphasizes on analyzing and comparing efficiencies of four different sets of three-qubit partially entangled states for teleportation and dense coding under noisy conditions. Our analysis shows some interesting observations regarding efficiencies of different sets of states and further sheds light on the complex nature of entanglement and nonlocality in presence of noise. We characterize nonlocal correlations in different sets of states through our modified operator using the Mermin inequality. Our results show that efficiencies of partially entangled three qubit states are in line with the existence of nonlocal correlations as identified by our modified operators and global quantum discord. The states are found to be efficient for controlled communication protocols even in the regions where the Svetlichny inequality is not violated by these states in presence and absence of noise. As against the general belief that more correlations in the input state may lead to better efficiency, our study suggests that less correlations in input state can be more useful for certain protocols, and therefore further sheds light on the complex nature of multiqubit entanglement, nonlocality and associated efficiency. Interestingly, for non-optimal weak measurement reversal operations, we identify states close to a product input state which lead to optimum efficiency for selected values of other parameters in the protocol.

  Extending our analysis from three qubit states to multiqubit states, in Chapter 6, we further address the efficacy of maximally and partially entangled multiqubit states in noisy environment for analyzing the fidelity and controller's power in a controlled teleportation protocol. Precisely, the chapter analyzes two sets of $(N+2)$-qubit partially entangled states for controlled teleportation protocol in noisy conditions where N represents number of controllers in the protocol. We further extend our analysis to study the authority of a controller on the protocol in relation to the degree of entanglement, nonlocality, strength of noise parameter, measurements performed by controllers and weak measurement parameters. Interestingly, we find that the average fidelity using a specific set of states as resources in ideal conditions depends only on the measurement performed by one controller, i.e., the efficiency of these states is independent of the state parameter and measurements performed by other $(N-1)$ controllers. This further paves a way for an experimental set-up with a lot of flexibility in terms of degree of entanglement of the shared resource and performing a single measurement from controller's perspective. Surprisingly, even when these set of states are subjected to noise and weak measurement operations, the average fidelity is always independent of measurements performed by $(N-1)$ controllers. Our analysis further shows that in noisy conditions, set of partially entangled states always result in better fidelity than the corresponding maximally entangled states. Further, for higher

values of weak measurement parameter, effects of noise can be suppressed efficiently to achieve optimal efficiency as in the case of an ideal channel.

1.8 THESIS OUTLINE

The remainder of this Thesis is organized as follows:

Chapter 2 presents an efficient operator to identify nonlocal correlations in two-qubit systems.
Chapter 3 proposes effective Bell-type operators for three-qubit quantum states.
Chapter 4 analyzes Bell-type operators for four- and five-qubit quantum states.
Chapter 5 demonstrates applications of partially entangled three qubit states for quantum teleportation and dense coding protocols in relation with entanglement and nonlocal correlation.
Chapter 6 illustrates the efficiencies of $(N+2)$-qubit partially entangled states for controlled teleportation protocols with the involvement of N controllers.
Chapter 7 concludes the Thesis followed by the bibliographic information.

…