Chapter 1

General introduction

In physical systems, correlations describe the covariations of one variable with another on average across space and time, and can be categorized in two different forms: classical correlation and quantum correlation. Classical correlation can be explained by the laws of classical physics. The other part, which can not be explained by the laws of classical physics is quantum correlation. Quantum correlations may be inherently probabilistic and nonlocal, whereas classical correlations can be described by local deterministic theories. One possible way to detect the existence of quantum correlations is through the violation of the gravitational weak equivalence principle for quantum systems.

Although quantum theory works mainly for atomic or subatomic particles, i.e., in microscopic scale, it may be extended to the macroscopic scale under suitable circumstances. The weak equivalence principle which is a famous property of classical systems is shown to be violated in the quantum domain. In some cases, classical properties of a particle will emerge in the macroscopic limit of quantum mechanics. As for example, the compatibility between the weak equivalence principle and the quantum mechanics is recovered in the macroscopic limit of the latter [Ali et al., 2006; Chowdhury et al., 2012].

From the practical point of view, in information theory quantum correlations have been used as resource in performing tasks that are unable to be achieved using classical means, leading to many interesting and important information-theoretic applications, such as dense coding, the violation of local uncertainty relation by nonlocal correlations, the sending of unknown quantum states at a distant location using finite resources in quantum teleportation, the generation of secret key
in quantum cryptography, better playoff of nonlocal games, i.e., Bell-CHSH game, etc. The different forms of uncertainty relations are one aspect of the conceptual difference between classical and quantum physics. However, the understanding of the exact difference between these two worlds is vital in learning how to perform different information processing tasks. Developments in quantum information theory for both discrete [Horodecki et al., 2009] as well as continuous variables [Weedbrook et al., 2012] have brought about the realization of subtle differences in various categories of correlations.

Among all the properties, nonlocality plays a key role in quantum theory. These non-classical, more specifically, nonlocal correlations can be categorised by three different forms, i.e., entanglement, steering and Bell-noncal correlations. For bipartite systems, steering is a kind of correlation, in the formulation of which at least one of the systems is being trusted as quantum system. In case of entanglement, both of the systems are being trusted as quantum, whereas in Bell nonlocal correlations, none of them needs to be trusted as quantum system. This leads to a hierarchy, in which entanglement is the weakest and Bell nonlocality is the strongest of the three form of correlations, and steering takes the intermediate position [Cavalcanti et al., 2009; Jones, Wiseman, and Doherty, 2007; Wiseman, Jones, and Doherty, 2007]. Bell nonlocal states constitute a strict subset of steerable states which, in turn, are a strict subset of entangled states. For the case of pure entangled states of two qubits, the three classes overlap.

1.1 Gravitational Weak Equivalence Principle

Starting from Newton’s version of the equivalence principle which includes the universality of free fall (UFF), the development of the statement of the weak equivalence principle is an important foundation of the general theory of relativity. Any violation of the weak equivalence principle for quantum systems would require the development of new theoretical physics, especially the attempts to connect gravity with quantum mechanics.
1.1.1 The Principle of Equivalence

The traditional equivalence principle is fundamentally both classical and local, and it is interesting to enquire how it is to be understood in quantum mechanics. In the famous gedanken experiment conceived by Galileo, the universality of the ratio between the gravitational and inertial masses had been studied with test bodies in free fall from the leaning tower of Pisa [Galilei, 1638]. The principle of equivalence states about this equivalence between the inertial mass and the gravitational mass:

\[ m_i \equiv m_g \equiv m. \]

With respect to the mechanical motion of particles, Einstein concluded that a state of rest in a sufficiently weak, homogeneous gravitational field is physically indistinguishable from a state of uniform acceleration in a gravity-free space. Einstein elevated this concept to become the Principle of Equivalence which is the foundation of the General Theory of Relativity. Quantum mechanically, this statement becomes [Bonse and Wroblewski, 1983], 'The laws of physics are the same in a frame with gravitational potential \( V = -mgz \) as in a corresponding frame lacking this potential but having a uniform acceleration \( g \) instead'.

Several tests have been performed to show the validity of the equivalence principle with classical test bodies such as very sensitive pendula or torsion balances. Even for quantum mechanical particles, the validity of the principle is also proved using gravity-induced interference experiments [Colella, Overhauser, and Werner, 1975; Peters, Chung, and Chu, 1999].

1.1.2 The Weak Equivalence Principle of quantum mechanics

The other alternative form of equivalence principle states that when all sufficiently small test bodies fall freely, they acquire an equal acceleration independent of their mass or constituent in a gravitational field. To obtain quantum analogue of this statement, it might be replaced by some principle such as [Holland, 1993], 'The results of experiments in an external potential comprising just a sufficiently weak, homogeneous gravitational field, as determined by the wave function, are independent of the mass of the system'. This statement is known as weak equivalence principle of quantum mechanics (WEQ).
The most familiar tests of the weak equivalence principle are experiments of the Eötvös-type [Eötvös, 1890; Eötvös, Pekar, and Fekete, 1922], which measure the gravitational acceleration of macroscopic objects.

### 1.1.3 Violation of the Weak Equivalence Principle of quantum mechanics

The evidence of existence of quantum correlations will be given by the violation of WEQ through the mass dependence of an experimentally measurable quantity in gravitational field. The violation of WEQ can be shown both experimentally and theoretically. Experimental evidence exists in the interference phenomenon associated with the gravitational potential in neutron and atomic interferometry experiments [Colella, Overhauser, and Werner, 1975; Peters, Chung, and Chu, 1999]. Theoretically, for a particle bound in an external gravitational potential, it is seen that the radii, frequencies and binding energy depend on the mass of the bound particle [Greenberger, 1968, 1983; Greenberger and Overhauser, 1979]. Viola and Onofrio [Viola and Onofrio, 1997] have studied the free fall of a quantum test particle in a uniform gravitational field. They have made a rough estimation of the fluctuations around the mean value of time of flight, which is shown to be dependent on the mass of the particle. Another quantum mechanical approach of the violation of WEQ was given by Davies [Davies, 2004] using a model quantum clock [Peres, 1980]. In other examples [Ali et al., 2006; Chowdhury et al., 2012], the violation of WEQ is shown for smaller mass particles due to the existence of quantum correlations. It can also be shown the emergence of WEQ for larger mass particles in the classical limit.

### 1.2 Uncertainty relations

Uncertainty principle is one of the most fundamental and important physical properties of quantum mechanics [Deutsch, 1983; Heisenberg, 1927; Kraus, 1987; Maassen and Uffink, 1988; Robertson, 1929]. It gives a fundamental limit to the precision of measurement outcomes for the measurement of two noncommuting observables, say, position and momentum on the observed quantum system, though there are several interpretations of this limit. Even with perfect instruments and
techniques, the uncertainty is inherent in the nature. In the derivation of uncertainty relation, the correlation of the observed system with the other system called quantum memory is not considered. If this correlation is considered, the precision of measurement outcome can be increased for the measurement of two noncommuting observables [Berta et al., 2010; Li et al., 2011; Pramanik, Chowdhury, and Majumdar, 2013; Prevedel et al., 2011]. For example, if the observed system is in maximally entangled state with the quantum memory, the uncertainty can be reduced to zero. Uncertainty relation is one of the aspects, which introduces a sharp distinction between classical and quantum physics in the sense that classical system can be assigned with its complete state without disturbing the system, whereas quantum mechanics denies this possibility due to the presence of uncertainty relation. There are several uncertainty relations on the basis of different methods of uncertainty measurement.

1.2.1 Heisenberg uncertainty relation and its generalization

In 1927, Werner Heisenberg first introduced the famous uncertainty relation [Heisenberg, 1927], where standard deviation is used as a measure of uncertainty. Heisenberg uncertainty relation (HUR) states that the position and momentum of a microscopic particle cannot be measured simultaneously with arbitrary precision, i.e., the more precisely the position of some particle is determined, the less precisely its momentum can be known, and vice versa. The formal inequality relating the standard deviation of position \(x\) and the standard deviation of momentum \(p\) was derived later by Kennard [Kennard, 1927] and Weyl [Weyl, 1928]. They proved that the inherent fluctuations of position and momentum are bounded by the Plank constant, which is mathematically given as

\[
\Delta x \Delta p \geq \frac{\hbar}{2},
\]

(1.1)

where \(\Delta x\) and \(\Delta p\) are the standard deviations of position and momentum respectively. \(\hbar (= h/2\pi)\) is the reduced Plank constant. The relation (1.1) is known as the famous Heisenberg uncertainty relation.
In 1929, Robertson [Robertson, 1929] generalized the inequality (1.1) for arbitrary observables. For the measurement of any pair of arbitrary noncommuting Hermitian operators, say, $\hat{A}$ and $\hat{B}$ on the system $\mathcal{S}$, Robertson modified the Heisenberg uncertainty relation as

$$\Delta \hat{A} \Delta \hat{B} \geq \frac{1}{2} \left| \langle [\hat{A}, \hat{B}] \rangle_{\rho_S} \right|,$$  \hspace{1cm} (1.2)

where the uncertainty of measurement outcomes for the measurement of an observable $\hat{O} \in \{\hat{A}, \hat{B}\}$ is given in terms of standard deviation as

$$\Delta \hat{O} = \sqrt{\langle \hat{O}^2 \rangle - \langle \hat{O} \rangle^2},$$  \hspace{1cm} (1.3)

and $\langle \hat{O} \rangle = \text{Tr} [\rho_S \hat{O}]$ is the expectation value of the observable $\hat{O}$ for the density state $\rho_S$ of the system $\mathcal{S}$. The commutation relation is given by $[\hat{A}, \hat{B}] := \hat{A} \hat{B} - \hat{B} \hat{A}$.

In 1930, Schrödinger [Schrödinger, 1930] further generalized the modified inequality (1.2) given by Robertson by adding a new term for quantum states for which the covariance of the two operators is non-zero and the generalized uncertainty relation is given by

$$(\Delta \hat{A})^2 (\Delta \hat{B})^2 \geq \frac{1}{2} \left| \langle [\hat{A}, \hat{B}] \rangle_{\rho_S} \right| + \left( \frac{1}{2} \left| \langle \{\hat{A}, \hat{B}\} \rangle_{\rho_S} \right| - \langle \hat{A} \rangle_{\rho_S} \langle \hat{B} \rangle_{\rho_S} \right),$$  \hspace{1cm} (1.4)

where the anticommutator $\{\hat{A}, \hat{B}\} := \hat{A} \hat{B} + \hat{B} \hat{A}$. For quantum states with zero covariance of $\hat{A}$ and $\hat{B}$, this relation (1.4) reduces to Robertson’s inequality (1.2).

In this sense, it is more general and can be applied to any two observables of a large class of states of quantum systems.

**Drawbacks:**

The uncertainty relations, defined on the basis of standard deviations of the corresponding conjugate pair of dynamical variables are meaningful, only if both the standard deviations are finite. There are a number of interesting statefunctions, whose standard deviation diverges. In fact, the use of variance as a measure of uncertainty is quite limited. Uncertainty in terms of variance of an observable gives the average uncertainty, where the average is taken over all possible measurement outcomes of the observable. Another and most important drawback is...
that both the lower limits of the inequalities (1.2) and (1.4) depend on the state of
the quantum system.

1.2.2 Entropic uncertainty relations

To improve the drawbacks of the variance-based uncertainty relations and also to
connect uncertainty with information-theoretic concepts, the uncertainty relating
to the outcomes of observables has been reformulated by Everett [Everett, 1973]
on the basis of information entropy. From the perspective of information theory,
uncertainty is nothing but the deficiency of information. He concluded that the
new relation is stronger than the variance-based relation, since it implies the former
but is not implied by the former. The entropic uncertainty relation (EUR) involves
sum of uncertainties measured in terms of Shannon entropy [Bialynicki-Birula and

Deutsch [Deutsch, 1983] first introduced the entropic uncertainty relation for two
observables. Later, the uncertainty relation was improved and the improved ver-
sion is given by

\[ H(R) + H(S) \geq \log_2 \frac{1}{c}, \tag{1.5} \]

which was first conjectured by Kraus [Kraus, 1987], and then proved by Maassen
and Uffink [Maassen and Uffink, 1988]. Here, \( H(X) = -\sum_i p_i \ln p_i \) denotes
the Shannon entropy of the probability distribution \( \{ p_i \} \) of the measurement
outcomes of observable \( X (X \in \{ R, S \}) \), \( p_i \) is the probability of the \( i \)th outcome
of the observable, and \( \frac{1}{c} \) quantifies the complementarity of the observable. For
nondegenerate observables,

\[ c = \max_{i,j} |\langle a_i | b_j \rangle|^2, \tag{1.6} \]

where \( |a_i\rangle \) and \( |b_j\rangle \) are eigenvectors of \( R \) and \( S \) respectively. The inequality
(1.5) is a more general form of the uncertainty relation containing correlations
in all orders of two observables of a discrete variable quantum system. In case
of continuous variable systems for example using the position and momentum
distribution of a quantum system, the entropic uncertainty principle first proposed
by Bialynicki-Birula and Mycielski is given by [Bialynicki-Birula and Mycielski,
1975]

\[ \mathcal{H}(X) + \mathcal{H}(P) \geq \ln \pi e. \]  

(1.7)

The advantage of these uncertainty relations over the variance-based relations is that both the lower bounds of the inequalities (1.5) and (1.7) are independent of the state of the system.

Recently, Berta et al. [Berta et al., 2010] have shown that the lower bound of entropic uncertainty relation (1.5) can be improved in the presence of quantum memory. They generalized the uncertainty relation as

\[ S(R|B) + S(S|B) \geq \log_2 \frac{1}{c} + S(A|B), \]  

(1.8)

where \( S(R|B) = S(\rho_{RB}) - S(\rho_B) [S(S|B)] \) is the conditional von Neumann entropy, which quantifies the uncertainty corresponding to the measurement \( R(S) \) on the system A given information stored in the system B (i.e., quantum memory). \( S(\rho) \) is the von Neumann entropy with \( \rho_{RB} \) denoting the state after \( R \) measurement on subsystem A of \( \rho_{AB} \) and \( \rho_B \) denoting the reduced state of \( \rho_{RB} \). \( S(A|B) \) quantifies the lower bound of the one-way distillable entanglement between Alice’s system and Bob’s system [Devetak and Winter, 2005].

Drawbacks:

As a measure of uncertainty, entropy gives average uncertainty of observables, where the average is again taken over all possible measurement outcomes of an observable similar to variance-based uncertainty. Entropic functions do not distinguish the uncertainty inherent in obtaining any combination of outcomes for different measurements.

1.2.3 Fine-grained uncertainty relation

To overcome the drawbacks of the uncertainty relations obtained in coarse-grained way, where all the measurement outcomes of an observable are considered and to capture the full nonlocal strength by quantum physics, Oppenheim and Wehner [Oppenheim and Wehner, 2010] have introduced a completely different and new form of the uncertainty relation known as fine-grained uncertainty relation (FUR). Here, uncertainty is measured for a particular measurement outcome or some
combination of outcomes to win a particular nonlocal game. The winning condition
is the essence of fine graining and every game gives rise to an uncertainty relation,
and vice versa. In discrete-variable systems, fine-grained uncertainty relation is
the strongest one.

In Ref. [Oppenheim and Wehner, 2010], Oppenheim and Wehner have considered
games for both the single qubit case and the bipartite case. In the single-qubit
system, a FUR can be described by the following game, where Alice is considered
to receive a binary question \( s \in \{0, 1\} \) with the probability \( p (s) = \frac{1}{2} \). When
she receives the question \( s = 0 \) (\( s = 1 \)), Alice measures \( \sigma_z \) (\( \sigma_x \)) observable on
her state \( \rho_A \). She gets outcome \( a_s \), where \( a_s \in \{0, 1\} \). Alice wins the game if
she gets a particular outcome \( a_s \) for both the questions \( s = 0 \) and \( s = 1 \). The
winning probability of the above game is given by

\[
P_{\text{game}} = \sum_s p(s) p(a_s) \rho_A \leq P_{\text{game}}^{\text{max}} = \max_{\rho_A} P_{\text{game}}^{\text{max}},
\]

where \( p(a_s) \) is the probability of obtaining a particular outcome \( a_s \) for the
measurement corresponding to the question \( s \) on the state \( \rho_A \). \( P_{\text{game}}^{\text{max}} \) is the maximum
winning probability over all possible strategies, i.e., the choice of the single-qubit
state \( \rho_A \) in this game. For spin-up outcome (i.e., \( a_s = 0 \)), \( P_{\text{game}}^{\text{max}} = \frac{1}{2} + \frac{1}{2\sqrt{2}} \)
occurs for the eigenstates of \( (\sigma_x + \sigma_z)/\sqrt{2} \). For the spin-down winning condition
(i.e., \( a_s = 1 \)), we achieve the same maximum winning probability using eigenstates
of \( (\sigma_x - \sigma_z)/\sqrt{2} \). These are known as maximally certain states.

For the bipartite case, authors have considered a game according to which Alice
and Bob both receive binary questions, i.e., projective spin measurements along
two different directions at each side. For this case if \( \rho_{AB} \) is a bipartite state shared
between Alice and Bob, the winning probability is given by the relation

\[
P_{\text{game}} (\mathcal{T}_A, \mathcal{T}_B, \rho_{AB}) = \sum_{t_A, t_B} p(t_A, t_B) \sum_{a,b} V(a, b|t_A, t_B) \langle (A^a_{t_A} \otimes B^b_{t_B}) \rangle_{\rho_{AB}} \leq P_{\text{game}}^{\text{max}},
\]

where \( \mathcal{T}_A \) and \( \mathcal{T}_B \) represent the set of measurement settings \( \{t_A\} \) and \( \{t_B\} \)
chosen by Alice and Bob, respectively, with probability \( p(t_A, t_B) \). Alice and
Bob receive their binary question \( t_A \) and \( t_B \), and their outcomes are \( a \) and \( b \),
respectively, with

\[
A^a_{tA} = \frac{1}{2} \left[ I + (-1)^a A_{tA} \right], \\
B^b_{tB} = \frac{1}{2} \left[ I + (-1)^b B_{tB} \right]
\]  

(1.11)

being a measurement of the observable \( A_{tA} \) and \( B_{tB} \), respectively. Here, \( V(a, b \mid t_A, t_B) \) is some function determining the winning condition of the game. The winning condition corresponding to a special class of nonlocal retrieval games (CHSH game) for which there exists only one winning answer for one of the two parties, is given by \( V(a, b \mid t_A, t_B) = 1 \), if and only if \( a \oplus b = t_A \cdot t_B \), and 0 otherwise. \( P_{\text{game}}^{\text{max}} \) is the maximum winning probability of the game, i.e.,

\[
P_{\text{game}}^{\text{max}} = \max_{T_A, T_B, \rho_{AB}} P_{\text{game}}(T_A, T_B, \rho_{AB}).
\]  

(1.12)

Using the maximum winning probability it is possible to discriminate among classical theory, quantum theory, and no-signaling theory with the help of the degree of nonlocality [Oppenheim and Wehner, 2010]. Later, it has been generalized for the tripartite systems [Pramanik and Majumdar, 2012]. Fine-grained uncertainty relation also provides an optimal lower bound of entropic uncertainty in presence of quantum memory [Pramanik, Chowdhury, and Majumdar, 2013]. Recently, fine-grained uncertainty relation is derived for continuous variable systems [Chowdhury, Pramanik, and Majumdar, 2015] and is demonstrated in the Chapter 5.

1.2.4 Applications

The presence of uncertainty relations endows quantum mechanics with significant advantages over classical mechanics for performing different information processing tasks. Various versions of uncertainty relations have been used to detect entanglement [Biswas and Agarwal, 2005; Gillet, Bastin, and Agarwal, 2008; Nha, 2007; Simon, 2000; Wehner and Winter, 2010], to classify mixedness of states [Mal, Pramanik, and Majumdar, 2013], to categorize different physical theories according to their strength of nonlocality [Dey, Pramanik, and Majumdar, 2013; Oppenheim and Wehner, 2010; Pramanik and Majumdar, 2012], and to bound information leakage in key distribution [Berta et al., 2010; Branciard et al., 2012; Devetak and Winter, 2005; Furrer et al., 2012; Grosshans and Grangier, 2002; Pramanik,
1.3 EPR paradox

At the advent of quantum mechanics, a point of view of quantum mechanics arose differentiating it from the classical view point. According to this view point [Nielsen and Chuang, 2000], an unobserved particle does not possess physical properties that exist independent of observation, unless otherwise an appropriate measurement is performed upon the system. For example, according to quantum mechanics a qubit does not possess definite properties of $\sigma_z$ and $\sigma_x$ observables, the spins in the $z$ and $x$ directions respectively, each of which can be revealed with certain probabilities for the possible measurement outcomes after performing the appropriate measurement on the observables. The most prominent objector was Albert Einstein. In 1935, Einstein in his famous ‘EPR paper’ [Einstein, Podolsky, and Rosen, 1935], in collaboration with Boris Podolsky and Nathan Rosen, proposed a thought experiment demonstrating that quantum mechanics is not a complete theory of Nature. They emphasized that any physical theory of nature must be complete if it includes ‘elements of reality’. The way they attempted to do the thought experiment was by introducing two assumptions,

1. **Reality**: If it is possible to predict with certainty (i.e., with probability 1) the value of a physical quantity of a system, without in any way disturbing the system, i.e., without performing any actual measurements, then there exists an element of reality corresponding to that physical quantity.

2. **Locality**: Performing a measurement on one system cannot have any influence on the result of measurements on the other.

These two assumptions together are known as the assumptions of **local realism**.

For example, a singlet state is shared between an entangled pair of qubits belonging to Alice and Bob, respectively. The singlet state is given by

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$  \hspace{1cm} (1.13)

They are assumed to be far enough apart from each other and they perform their measurements simultaneously. Now, if Alice measures $\sigma_z$ observable on her qubit and gets spin up outcome, then she can predict with certainty (probability 1) what
Chapter 1. *General introduction*

will be the Bob’s measurement outcome if he would measure the same observable on his qubit. So, Alice can predict that Bob will get spin down outcome. Again, if she obtains spin down outcome, Bob’s outcome will be spin up. Therefore, \( \sigma_z \) is the element of reality as it is possible to predict the certain value of this observable, immediately before the measurement on Bob’s qubit. Similarly, \( \sigma_x \) is also an element of reality, for which both the observables \( \sigma_z \) and \( \sigma_x \) can be measured simultaneously with arbitrary precision for Bob’s system. This phenomenon, which contradicts the uncertainty relation given by Heisenberg [Heisenberg, 1927], appears as a paradox. According to the uncertainty relation, \( \sigma_z \) and \( \sigma_x \) are two noncommuting observables. So, they can not be measured simultaneously with arbitrary precision. This paradox is known as EPR paradox. But Einstein did not challenge the uncertainty relation. EPR wanted to show that the quantum mechanical description of physical reality given by wave functions is incomplete, by demonstrating that quantum mechanics lacked some essential element of reality, by their criterion.

EPR explained the paradox as the information about the outcome of all possible measurements was already present in both particles. Also the more complete theory contains variables corresponding to all the elements of reality. So, there were some ‘hidden variables’, which encoded that information. Then they concluded that quantum mechanics was incomplete since its formalism does not permit hidden variables. In 1964, John Bell [Bell, 1964] showed that quantum mechanics and the class of hidden variable theories Einstein favoured (local hidden variable theory) would lead to different experimental results. There are many experiments to test Bell’s theorem, e.g., those of A. Aspect and others [Aspect, Dalibard, and Roger, 1982; Aspect, Grangier, and Roger, 1981, 1982]. They support the predictions of quantum mechanics rather than the local hidden variable theories supported by Einstein. Realist interpretation of quantum mechanics must reject either locality or realism.

### 1.4 Classification of entanglement

In EPR paradox [Einstein, Podolsky, and Rosen, 1935], it appears that one particle somehow knows what measurement has been performed on the other particle, and with what outcome, even though there is no known means for communication of such information between the particles. The word ‘entanglement’ was first
coined by Schrödinger [Schrödinger, 1935, 1936] to describe the property of such spatially separated but quantum mechanically correlated particles. Entanglement is a physical phenomenon which occurs in quantum domain. If a pairs or groups of particles are entangled, then each particle can not be fully described by quantum mechanics without considering the other.

Quantum systems can become entangled through various types of interactions such as using spontaneous parametric down conversion, fiber coupler, quantum dots, entanglement swapping etc. Even though two particles are presently not interacting (interacted once before) and also remote from one another, then they still may be entangled if their shared state can not be written as the mixture of product of the states of individual subsystems. Entanglement is broken through the interaction of the entangled particles with the environment (decoherence).

There are two types of entangled states: pure entangled and mixed entangled. For the bipartite case, let us consider two particles A and B associated with finite dimensional Hilbert spaces $H_A$ and $H_B$, respectively. The state space of the composite system is given by the tensor product $H = H_A \otimes H_B$.

### 1.4.1 Pure entangled states

Consider, $|\psi\rangle (\in H_A \otimes H_B)$ be the pure state of the composite system, and $|\psi\rangle_A$ and $|\psi\rangle_B$ are that of the subsystems A and B, respectively. $|\psi\rangle$ is said to be separable state, if it can be written in the form

$$|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B .$$

When the composite pure state can not be written in this form, i.e., in the form of the product of individual states of subsystems, it is called entangled state. When a pair of systems share an entangled pure state, it is not possible to assign states to individual systems. In general, a bipartite pure state is entangled if and only if its reduced states are mixed rather than pure. The more uncertainty statistically will cause larger entropy. So, the zero entropy of a composite pure state indicates that there is no uncertainty about a system in pure state, whereas the entropy of each subsystem of the composite system gives maximum entropy for $2 \times 2$ mixed states.
For the case of multipartite system, let a composite system, consisting of \( n \) sub-systems has state space \( H = H_1 \otimes \ldots \otimes H_n \). A pure state \( |\psi\rangle (\in H) \) is said to be entangled if
\[
|\psi\rangle \neq |\psi\rangle_1 \otimes \ldots \otimes |\psi\rangle_n,
\]
where \( |\psi\rangle_i \) is a pure state of the \( i \)-th subsystem.

### 1.4.2 Mixed entangled states

Let us consider bipartite mixed state case. A mixed state of the composite system is described by density matrix \( \rho \) acting on the Hilbert space of the composite system, \( H = H_A \otimes H_B \). When there is less than total information about the state of a quantum system, we need density matrices to represent the state. The density matrix of a pure state \( |\phi\rangle \) is described by the outer product, \( \rho_\phi = |\phi\rangle \langle \phi| \). For separable mixed states, \( \rho \) can be written as
\[
\rho = \sum_k p_k \rho_A^k \otimes \rho_B^k,
\]
where \( p_k \geq 0 \) and \( \sum_k p_k = 1 \); \( \{\rho_A^k\} \) and \( \{\rho_B^k\} \) are the pure ensembles of the respective subsystems. It is clear from the definition that the family of separable states is a convex set. \( \rho \) is said to be entangled if it can not be written in the form given above, i.e., it can not be written as the mixture of product states of individual systems. A mixed state with rank 1 describes a pure ensemble.

For a multipartite system consisting of \( n \) subsystems, a mixed state \( \rho \) acting on the state space \( H (= H_1 \otimes \ldots \otimes H_n) \) of the composite system is said to be entangled if
\[
\rho \neq \sum_k p_k \rho_1^k \otimes \ldots \otimes \rho_n^k,
\]
where \( \rho_i^k \) is the pure ensemble of \( i \)-th subsystem.
1.4.3 Applications

Entanglement has many applications in quantum information-processing tasks that can not be achieved by any other means. Superdense coding and quantum teleportation are two important applications of entanglement. Technologies relying on quantum entanglement are now being developed. In quantum cryptography, entangled particles are used to transmit signals that can not be eavesdropped upon without leaving a trace. In quantum computation, entangled quantum states are used to perform computations in parallel, which may allow certain calculations to be performed much more quickly than they ever could be with classical computers.

1.5 Classification of steering

In the pioneering work of Einstein, Podolsky and Rosen (EPR) [Einstein, Podolsky, and Rosen, 1935], EPR argued that the quantum mechanical description of the state of a particle is not complete, when one considers a position-momentum correlated state of two particles, and assumes the notions of spatial separability, locality, and reality to hold true at the level of quantum particles. This is arguably a paradoxical feature of quantum mechanics and is well known as EPR paradox. An immediate consequence of correlations between spatially separated particles was then noted by Schrödinger [Schrödinger, 1935, 1936] in that it allowed for the control of the state on one side merely by the choice of the measurement basis on the other side without in any way having direct access to the affected particle. So, the EPR paradox was reexpressed as the possibility of steering by Schrödinger. This is also known as EPR steering.

Uncertainty relations are linked directly to the ability of quantum states to enable steering. Starting with the Heisenberg uncertainty relation, a number of improved uncertainty relations have been provided [Bialynicki-Birula and Mycielski, 1975; Maassen and Uffink, 1988; Oppenheim and Wehner, 2010; Robertson, 1929; Schrödinger, 1930; Wehner and Winter, 2010]. Again, stronger steering criteria are built up with the help of stronger uncertainty relations. To capture steering of an entangled state, one needs to built up some steering inequalities using uncertainty relations.
1.5.1 The Reid criterion for steering

The phenomenon of quantum steering [Schrödinger, 1935, 1936] emerging from the EPR paradox [Einstein, Podolsky, and Rosen, 1935] was first formulated by Reid for experimental realization [Reid, 1989]. She proposed the EPR steering criterion for continuous variable systems based on the position-momentum Heisenberg uncertainty relation, in terms of an inequality involving products of inferred variances of incompatible observables. For two conjugate observables $\hat{X}_1$ and $\hat{X}_2$, which are noncommuting, the Reid inequality is given by

$$\left( \Delta_{\text{inf}} \hat{X}_1 \right)^2 \left( \Delta_{\text{inf}} \hat{X}_2 \right)^2 \geq 1,$$

where $\Delta_{\text{inf}} \hat{X}_i$ is the variance of the inferred observables $\hat{X}_i$ [$i \in \{1, 2\}$]. For a given bipartite entangled state, the violation of the above inequality will give the EPR steering of that state. Ou et al. [Ou et al., 1992] gave an experimental demonstration of the EPR paradox for the case of two spatially separated and correlated light modes. The EPR criterion has been used to demonstrate the steerability of two mode squeezed vacuum states [Steinlechner et al., 2013] experimentally and entanglement in Bose-Einstein condensates, as well [He et al., 2012, 2011; Opanchuk et al., 2012]. Other works have shown that the Reid inequality is effective in giving demonstration of the EPR paradox for systems in which correlations appear at the level of variances.

**Drawback:**

The steerability of the states having correlations higher than the second order remains unable to be captured by the Reid criterion for EPR steering, although the Bell nonlocal correlation for that states may be exhibited [Chowdhury et al., 2014; Walborn et al., 2011]. In Chapter 4, the failure of the Reid criterion is demonstrated for some non-Gaussian states.

1.5.2 The entropic steering criterion

To improve the situation produced by the Reid criterion for EPR steering and to derive more stronger steering inequality, in terms of an information-theoretic task Walborn et al. [Walborn et al., 2011] have introduced a new steering criterion
on the basis of more general entropic uncertainty relation proposed by Bialynicki-Birula and Mycielski [Bialynicki-Birula and Mycielski, 1975]. Entropic functions by definition incorporate correlations up to all orders. They have considered that the measurements correspond to either position or momentum. For steerable states, correlations between the measurement outcomes of Alice and Bob can not be explained by a local hidden state (LHS) model. So, for continuous variable systems, the entropic steering inequality can be written as the sum of conditional Shannon entropies [Walborn et al., 2011]

\[ h(X_B | X_A) + h(P_B | P_A) \geq \ln \pi e, \]  

(1.19)

where \( X_A, X_B \) are the correlated positions and \( P_A, P_B \) are the correlated momenta of the particles possessed by Alice and Bob, respectively. The EPR steering criterion (1.18) derived by Reid [Reid, 1989] can be obtained as a limiting case of the entropic steering criterion (1.19). The new criterion can be used to show steerability not only for Gaussian states having correlations up to second order but also for pure entangled non-Gaussian states [Walborn et al., 2011], for which Reid criterion fails to detect steerability. Since entanglement is a weaker form of correlations compared to steering [Cavalcanti et al., 2009; Wiseman, Jones, and Doherty, 2007], it is clear that for such entangled non-Gaussian states the steering correlations appear at the level of higher than the second order (variances). Therefore, the criterion (1.19) is more sensitive than the Reid criterion (1.18). Chapter 4 includes the steerability of some class of entangled non-Gaussian states through the entropic steering criterion [Chowdhury et al., 2014].

For discrete variable systems, the lower bound of the entropic steering inequality (1.19) will be changed according to the discrete version of the entropic uncertainty relation given by the inequality (1.5). In terms of conjugate pairs of discrete variables \( \{R_A, S_A\} \) and \( \{R_B, S_B\} \), the entropic steering inequality can be written as [Schneeloch et al., 2013]

\[ \mathcal{H}(R_B | R_A) + \mathcal{H}(S_B | S_A) \geq \log_2 \frac{1}{c_B}, \]  

(1.20)

Here, the correlations exist between \( R_A \) and \( R_B \) (\( S_A \) and \( S_B \)), and \( c_B \) is the value of \( c \) given by the Eq.(1.6) associated with the observables of Bob’s system. The steerability is to be shown through the violation of the steering inequalities (1.19) and (1.20).
Drawback:

Although entropic steering criterion overcomes the drawbacks of Reid criterion for steering, it has also some drawbacks itself. In continuous variable systems, there are some non-Gaussian states like NOON states, for which entropic steering criterion detects steerability only with \( N = 1 \) [Chowdhury et al., 2014]. But for \( N \geq 2 \), these states are not steerable through the entropic criterion in spite of violating Bell-type inequalities for all \( N \) [Bell, 1964; Clauser et al., 1969; Wildfeuer, Lund, and Dowling, 2007]. So, NOON states should be steerable for all values of \( N \) since steering lies between entanglement and nonlocality in the hierarchy [Wiseman, Jones, and Doherty, 2007] of quantum correlations.

1.5.3 The fine-grained steering criterion

The tightest steering inequality in discrete variable systems is obtained [Pramanik, Kaplan, and Majumdar, 2014] through the application of the fine-grained uncertainty relation (FUR), first proposed by Oppenheim and Wehner [Oppenheim and Wehner, 2010]. Fine-graining makes it possible to distinguish the uncertainty inherent in obtaining any particular combination of outcomes for different measurements. They bound an event corresponding to win a nonlocal retrieval game considered between Alice and Bob by its minimum possible uncertainty, or maximum possible certainty, for two incompatible observables. In discrete variable systems, fine-grained uncertainty relation given by the inequality (5.3) is the strongest uncertainty relation. If the combined state between Alice and Bob is steerable, Alice’s measurement outcome \( a \) for the measurement chosen randomly from the set \( A \in \{ S, T \} \) and Bob’s measurement outcome \( b \) for the measurement chosen randomly from the set \( B \in \{ P, Q \} \) can not be written in terms of local hidden state (LHS) model. So, For discrete variable systems, the fine-grained steering inequality is given by the sum of conditional probabilities [Pramanik, Kaplan, and Majumdar, 2014]

\[
P (b_P | a_S) + P (b_Q | a_T) \ > \ 1 + \frac{1}{\sqrt{2}},
\]  

where Alice has prior knowledge of Bob’s measurement settings. The steerable states must satisfy the inequality (1.21). The new steering inequality (1.21) improves over previous ones since it can experimentally detect all steerable two-qubit
Werner state considering only two measurement settings on each side and it is also able to show that pure entangled states are maximally steerable as well [Pramanik, Kaplan, and Majumdar, 2014].

For continuous variable systems, the improved version of steering criterion over the inability of the entropic criterion to show the steerability of NOON states for \( N \geq 2 \) is introduced in Chapter 5 based on newly derived fine-grained uncertainty relation using continuous variables [Chowdhury, Pramanik, and Majumdar, 2015].

### 1.6 Bell nonlocality

Inspired by the early works of EPR and Schrödinger, Bell was the first who proposed a new formalism [Bell, 1964; Clauser et al., 1969] for quantifying the correlations in terms of joint measurements of observables corresponding to two spatially separated particles for the case of any general theory obeying the tenets of locality and realism, and derived Bell’s inequality. Bell’s theorem brings a compelling example of an essential difference between quantum and classical physics. It states that any physical theory of local hidden variables can not reproduce all the predictions of quantum mechanical theory.

To obtain Bell’s inequality, it is considered that Charlie prepares a pair of particles A and B in a combined state \( \rho_{AB} \). He sends particle A to Alice and particle B to Bob. He repeats this process many times. After receiving her particle, Alice could choose to measure randomly one of two different observables labelled by \( A_1 \) and \( A_2 \). Similarly, Bob is capable of measuring randomly one of two different observables \( B_1 \) and \( B_2 \). The measurement of each observable has dichotomic outcomes yielding either the value +1 or −1. It is assumed that Alice and Bob are far enough apart from each other and perform their measurements simultaneously. Therefore, performing a measurement on one system can not have an influence on the result of measurements on the other system since any physical influence can not propagate faster than light. Considering these, Bell’s inequality is given by

\[
| \langle A_1 \otimes B_1 \rangle + \langle A_1 \otimes B_2 \rangle + \langle A_2 \otimes B_1 \rangle - \langle A_2 \otimes B_2 \rangle | \leq 2. 
\]  

(1.22)

This is also known as Bell-CHSH inequality [Clauser et al., 1969]. The above inequality is upper bounded by 2 under local hidden variable (LHV) theory. Bell-nonlocal correlations are those for which at least any Bell’s inequality is violated.
indicating nonexistence of LHV model. In deriving Bell’s inequality, quantum mechanics is not considered at all, only probability theory is invoked. So, Bell-nonlocal correlations are the strongest one in quantum mechanics. As for example [Nielsen and Chuang, 2000], we consider that Alice and Bob share singlet state given by the Eq.(1.13), which is maximally entangled state. If they perform measurements of the following observables:

\[ A_1 = Z_1 \]
\[ A_2 = X_1 \]
\[ B_1 = \frac{-Z_2 - X_2}{\sqrt{2}} \]
\[ B_2 = \frac{Z_2 - X_2}{\sqrt{2}} \],

(1.23)

the value of the Bell sum will become \(2\sqrt{2}\), which is the maximum Bell violation in quantum mechanics. So, quantum mechanics does not allow LHV theory. It turns out that Nature experimentally agrees with quantum mechanics. To derive his famous inequality, Bell considered two assumptions, which are 1) Reality and 2) Locality. Therefore, at least one of the assumptions is violated by quantum mechanics. It is possible to infer that violation of Bell’s inequality is due to the presence of nonlocal character of quantum mechanics known as “quantum entanglement”. Bell’s inequality was shown to be violated in quantum mechanics in several subsequent experiments [Aspect, Dalibard, and Roger, 1982; Aspect, Grangier, and Roger, 1981, 1982].

### 1.7 The utility of the Wigner function in continuous-variable systems

Quasiprobability distributions are mathematical objects, which satisfy several general features of ordinary probability distributions. Quasiprobability distributions arise naturally to study the phase space representation of quantum mechanics on top of the operator mechanics and are commonly used in quantum optics, time-frequency analysis [Cohen, 1995], and elsewhere. In this representation, the expectation values and probabilities of physical quantities are evaluated by rules of the classical statistics. In contradiction to the ordinary probabilities, some quasiprobability distributions have regions of negative probability density. When
the density operator is represented in a diagonal form, i.e., with respect to an over-
complete basis, then it can be written in a way more like an ordinary function, at
the expense that the function has the features of a quasiprobability distribution,
evolution of which completely determines the evolution of the system.

There exists a family of different quasiprobability distributions, depending on dif-
ferent operator orderings. The most important of these in the general physics
literature is the Wigner quasiprobability distribution [Wigner, 1932] introduced
by E. P. Wigner in 1932, which is related to symmetric operator ordering given by
the Weyl transform. In constructing the possible phase-space distribution, he had
to give up the positivity property of the distribution for states, which have no clas-
sical model. Thus the Wigner distribution could be negative, which is a convenient
indicator of quantum mechanical interference. The formalism of Wigner theory
demonstrates an autonomous description of the quantum world. The Wigner func-
tion, which yields the correct marginal distributions for a quantum system, is in
one hand the phase space counterpart of the density matrix and the quantum
counterpart of the classical distribution function on the other hand. Both states
and observables are represented by functions of the phase space coordinates. This
function is very useful in a variety of fields as it always exists but remarkably
used in quantum optics, particularly in the characterization and visualization of
nonclassical fields.

The fully symmetric Weyl order contains some of the basic properties of a char-
acteristic function of a probability distribution [Tatarskii, 1983]. So, the Wigner
quasiprobability distribution can be written in terms of characteristic function,
from which all quantum mechanical expectation values can be derived. Also, it is
well known that a probability distribution is nothing but the Fourier transform of
the characteristic function. Therefore, the Wigner function is defined as

\begin{equation}
W(\alpha) = \frac{1}{\pi^2} \int d^2 \beta \, \text{Tr} [ \rho D(\beta) ] \, \exp \left[ - (\beta \alpha^* - \beta^* \alpha) \right],
\end{equation}

which is a two-dimensional Fourier transform of the quantum mechanical charac-
teristic function

\begin{align}
\text{Tr} [ \rho D(\beta) ] &= \langle D(\beta) \rangle, \\
D(\beta) &= \exp [ \beta a^\dagger - \beta^* a ].
\end{align}
Here, $D(\beta)$ is the displacement operator for the complex phase-space displacement $\beta$, and $a$ and $a^\dagger$ are the annihilation and creation operators, respectively with the commutation relation $[a, a^\dagger] = 1$. $\rho$ is the density matrix of the respective quantum system. The Wigner function should be normalised, i.e.,

$$\int W(\alpha) \, d^2\alpha = 1.$$ (1.26)

This is a real, square integrable function and also remains bounded.

Banaszek and Wodkiewicz [Banaszek and Wodkiewicz, 1998, 1999] have used the two mode Wigner function instead of joint probability to derive the Bell like inequality in continuous variable systems. This becomes possible because they were able to express the Wigner function as an expectation value of a product of displaced parity operators and the parity plays the same role as spin-$1/2$ observables in discrete variable systems due to the property of getting dichotomic outcomes of both the observables.

In addition to the Wigner representation of phase-space defined above, there are many other quasiprobability distributions that arise in alternative representations of the phase space distribution, e.g., Glauber P, Husimi Q distributions. These representations are all interrelated to each other.

### 1.8 Quantum cryptography and quantum key distribution protocols

Quantum cryptography is the study to perform cryptographic tasks, i.e., the techniques for secure communication of encrypted messages in presence of third party by exploiting quantum mechanical properties. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are impossible to be performed using only classical communication. The best known and developed application of this is quantum key distribution, which offers an information-theoretic secure solution to the key exchange problem.

Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. In quantum key distribution protocol, the two communicating users, Alice and Bob share a random secret key, which remains unknown to any
third party, say, Eve trying to gain the knowledge of the key. This is achieved by Alice encoding the bits of the key as quantum data and sending them to Bob. The fundamental aspect of quantum mechanics says that the measurement on a quantum state in general changes the state except for the eigenstates of a system. Therefore, the very act of reading the data encoded in a quantum state by Eve must in some way measure it, introducing detectable anomalies. This will make Alice and Bob able to detect the presence of an eavesdropper. This is an important and unique property of QKD. The secret key can be used to encrypt messages by the sender (Alice) and decrypt messages by the receiver (Bob).

If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure, i.e., the eavesdropper has no information about it, otherwise no secure key is possible and communication is aborted. In contradiction with the classical key distribution, the security of QKD can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper. This is usually described as unconditional security, although there are some minimal assumptions required including that the laws of quantum mechanics apply and that Alice and Bob are able to authenticate each other.

Quantum key distribution is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel.

QKD exploits certain properties of information-encoded quantum states to ensure its security. There are two main categories of QKD depending on which property they exploit: prepare and measure protocols, and entanglement based protocols. The examples of both the protocols described below use discrete variable coding. Each of these two approaches can be further divided into three families of protocols: discrete variable, continuous variable and distributed phase reference coding. Among them, discrete variable protocols are the most widely implemented. The other two families are mainly concerned with overcoming practical limitations of experiments.
1.8.1 Prepare and measure protocols

This is based on quantum indeterminacy (i.e., measuring an unknown quantum state changes that state in some way), which underlies the results of Heisenberg uncertainty principle, information-disturbance theorem and no cloning theorem. This property can be used as a resource to detect eavesdropping if any and to calculate the amount of information that has been intercepted. The example of this type of protocols is BB84 protocol, which is first proposed by Bennet and Brassard in 1984 [Bennett and Brassard, 1984], and which is described below.

**BB84 Protocol:**

Assume that Alice and Bob wish to exchange a message securely. Alice initiates the message by sending Bob a secret key, which will be the mode for encrypting the message data. Eve has the objective to obtain some information about this secret key. Consider that Alice and Bob have access to a noiseless quantum channel and also a classical authenticated channel. Eve can act freely on the quantum channel as she has total access to the quantum channel, keeping in mind that she would be able neither to duplicate the quantum information (No-Cloning theorem) nor to measure a quantum state completely (Heisenberg uncertainty relation). But she can only listen to what happens on the classical channel, which makes her impossible to modify the information sent through the classical channel.

Alice chooses a random measurement basis from $\mathcal{B}_0$ and $\mathcal{B}_1$ given by

$$
\mathcal{B}_0 = \{ |0\rangle, |1\rangle \} \quad \text{and} \quad \mathcal{B}_1 = \left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}, \quad (1.27)
$$

which are $\sigma_z$ and $\sigma_x$ bases, respectively and also chooses a bit at random from $\{0, 1\}$. If the bit is 0, she sends the first state of her bases to Bob, if it is 1 she sends the second state of her bases. She repeats this procedure $N$ times and sends the $N$ resulting states to Bob.

After receiving all the states, Bob measures them randomly either in $\mathcal{B}_0$ or in $\mathcal{B}_1$ basis. He obtains $N$ bits string, known as raw key after performing measurements on $N$ states. Next, Alice and Bob announce their individual measurement basis through the classical communication channel but not the results they obtained.
When both the bases match with each other, they keep the corresponding bit of their string. When they differ, they discard the corresponding bit. Therefore, they obtain a string of \( n \) bits, which is smaller than \( N (n < N) \) that they agree on (called the sifted key). This is the secret key shared between Alice and Bob. Whenever Eve introduces errors to know about the key, Alice and Bob can notice it easily as their respective sifted key would differ, so that any subsequent communication making use of it to encrypt and decrypt messages would fail.

The goal of this protocol is to make sure that the knowledge of Eve about a secret key shared between Alice and Bob is very small. So, with high probability, either Alice and Bob will agree on a key about which Eve’s knowledge is very small, or Alice and Bob will decide to abort the key and try again, possibly with a different quantum channel as the security of the key cannot be guaranteed. In order to bound Eve’s knowledge about their secret key, Alice and Bob can apply a Privacy Amplification scheme [Bennett et al., 1995; Deutsch et al., 1996].

### 1.8.2 Entanglement based protocols

For an entangled state, measurement on one object affects the other. If Alice and Bob share an entangled state, anyone intercepting either object alters the overall system, revealing the presence of the third party and the amount of intercepted information. Here, entanglement can be used as a resource. The example of this type of protocols is E91 protocol, which is described below.

#### E91 Protocol :

In 1991, Ekert [Ekert, 1991] first proposed that quantum key distribution be implemented using the quantum states. This protocol is a modification of original Bennet-Brassard protocol and takes into consideration of EPR states. Let us consider that after preparing an entangled pair of spin-1/2 particles by a source, one particle is sent to Alice and other is sent to Bob. The state shared between Alice and Bob is maximally entangled, e.g., spin-singlet state given by the Eq.\((1.13)\).

If the particles are travelling along the \( z \)-direction, the measurement basis vectors of Alice and Bob are defined as being located in the \( x - y \) plane perpendicular to the trajectory of the particles. Alice randomly chooses to measure the spin
of incoming particles from the set of basis \( \{ A_1 = \sigma_x, A_2 = \frac{\sigma_x + \sigma_y}{\sqrt{2}}, A_3 = \sigma_y \} \) and similarly, Bob measures randomly chosen from the set \( \{ B_1 = \frac{\sigma_x + \sigma_y}{\sqrt{2}}, B_2 = \sigma_y, B_3 = -\frac{\sigma_x + \sigma_y}{\sqrt{2}} \} \). All the steps of this process is repeated for \( N \) times. After performing \( N \) measurements by both Alice and Bob, they publicly discuss about their measurement basis chosen for each particular measurement. They separate the measurements in two groups. In the first group, they accumulate the measurements performing in incompatible bases and the second group consist of measurements performing with compatible bases.

The correlation coefficient of joint measurements for the choice of Alice’s basis \( A_i \) and Bob’s basis \( B_j \) is given by

\[
C(A_i, B_j) = P_{++}(A_i, B_j) + P_{--}(A_i, B_j) - P_{+-}(A_i, B_j) - P_{-+}(A_i, B_j),
\]

(1.28)

where \( i, j = 1, 2, 3 \). \( P_{\pm\pm}(A_i, B_j) \) is the joint probability of getting the result \( \pm 1 \) for Alice’s choice of spin measurement \( A_i \) and of getting the result \( \pm 1 \) for Bob’s choice of spin measurement \( B_j \). If Alice and Bob choose incompatible bases to measure their respective particles, only then they publicly announce the actual measurement results they obtained and can figure out the value of the Bell sum, which can be written in terms of correlation coefficients of joint measurements as

\[
B = C(A_1, B_1) - C(A_1, B_3) + C(A_3, B_1) + C(A_3, B_3).
\]

(1.29)

Using local realism, Bell proved that \( |B| \leq 2 \). For maximally entangled states [Eq.(1.13)], \( |B| = 2\sqrt{2} \), i.e., violation of Bell’s theorem occurs. In absence of an eavesdropper, \( |B| \) should be equal to \( 2\sqrt{2} \). This assures Alice and Bob that when Alice and Bob choose compatible bases, their measurement results will be anti-correlated and can be converted into a secret string of bits, i.e., the key. The 1/3 chance that Alice and Bob will choose compatible bases to measure the incoming particles can shrink the key down to 30% of its original size, leaving them with a sifted key, which may be used in a conventional cryptographic communication between Alice and Bob. Within the sifted secret key, the spin up and spin down states of the particles correspond to bit values 0 and 1, respectively.

The entanglement present between Alice and Bob makes an eavesdropper, say, Eve hard to gain information about the key. The information about a system does not exist until an actual measurement has been performed on the system and
then communicated publicly. To know the key, Eve can provide a state, which is entangled with Alice’s and Bob’s system but Alice and Bob do not receive their expected value of $B$. So, in presence of an eavesdropper, $|B| < 2\sqrt{2}$. Future real life situations is more accurately indicated by the Ekert protocol as a practical implementation of quantum cryptography would involve a central source to overcome the distance limitations.

### 1.9 Non-Gaussian states and their usefulness

There exist both the theoretical and experimental demonstrations of all the quantum properties using Gaussian states. But it is realized that Gaussian states are a rather special class of states and it is quite difficult to achieve such special states experimentally. Gaussian states are defined as those states described by a Gaussian Wigner function, which differs from the non-Gaussian nature of the Wigner function of non-Gaussian states. The non-Gaussian states can be generated in different procedures, e.g., by truncating the Gaussian distribution or by the processes of photon subtraction and addition [Agarwal, 2013], and these states generally have a higher degree of entanglement than the Gaussian states. Also, non-Gaussian state can be constructed by the superposition of the Gaussian states. As for example, entangled non-Gaussian states can be constructed by the superposition of the energy eigenstates of the two-dimensional harmonic oscillator. Schrödinger’s cat states, some mixtures of squeezed or coherent states etc. are also the examples of non-Gaussian states.

As the non-Gaussian states are rich in entanglement than the Gaussian states, the former have applications in tests of Bell inequalities, quantum teleportation and other quantum information protocols [Lee et al., 2011; Lloyd and Braunstein, 1999; Opatrny, Kurizki, and Welsch, 2000; Seshadreesan, Dowling, and Agarwal, 2015; Takahashi et al., 2010]. Extensions of the entanglement criteria for non-Gaussian states have been proposed recently [Ivan et al., 2011; Roncaglia, Montorsi, and Genovese, 2014]. Non-Gaussianity is needed for entanglement distillation and quantum computation. Since the steering of correlated systems has started being studied only recently, and EPR steering for Gaussian states has been studied extensively both theoretically and experimentally, now it becomes important to understand the steering of systems with non-Gaussian correlations. A particular example of a non-Gaussian state was considered by Walborn et al. [Walborn
et al., 2011] revealing steering through the entropic inequality. Non-Gaussian entanglement and steering have also been recently studied in the context of Kerr-squeezed optical beams [Olsen and Corney, 2013].

1.10 Outline of thesis

In this thesis, some properties of quantum mechanics are studied using several classes of important non-Gaussian states for continuous variable systems. The outline of this thesis, which actually points towards the fact that non-Gaussian states are more nonlocal, is briefly given below.

In Chapter-2, we have studied the mass dependence of both the position detection probabilities for quantum particles projected upwards against gravity around the classical turning point and the point of initial projection, and also the mean arrival time of freely falling particles, using a class of non-Gaussian wave packets, which depart from the Gaussian wave packet by a continuous and tunable parameter. We have shown the stronger violation of the WEQ by increasing the non-Gaussian parameter of the wave packet through the mass dependence of the probabilities and the mean arrival time [Chowdhury et al., 2012]. Then, we have used a selection of Bohm trajectories to illustrate these features in the free fall case.

In Chapter-3, we have considered Laguerre-Gaussian beam, which is a classical optical beam with topological singularities and possesses Schmidt decomposition. We have shown that such classical beams share many features of two mode entanglement in quantum optics. We have demonstrated the coherence properties of such beams through the violations of Bell’s inequality for continuous variables using Wigner function formalism due to the presence of correlations between two different modes of the beam. The magnitude of the Bell violation is shown to be increased with higher orbital angular momenta of the vortex beam [Chowdhury, Majumdar, and Agarwal, 2013]. So, we have shown the mathematical reinterpretation of quantum nonlocality in classical theory.

In Chapter-4, we have demonstrated the steerability of several classes of currently important non-Gaussian entangled states [Chowdhury et al., 2014], such as the two-dimensional harmonic oscillator, the photon-annihilated two mode squeezed vacuum, and the NOON states for $N = 1$ only, through the violation of the entropic steering inequality. We have shown that the steerability of those states remains
unable to be captured by the Reid criterion, whereas that of Gaussian states is demonstrated using the Reid criterion. We have also provided a comparative study of violation of the Bell inequality for these states, from which it is shown that the entanglement present is more easily revealed through steering compared to Bell violation for several such states.

In Chapter-5, we have derived a fine-grained uncertainty relation for the measurement of two incompatible observables on a single quantum system of continuous variables, and have shown that continuous variable systems are more uncertain than discrete variable systems. Using the derived fine-grained uncertainty relation, we have formulated a stronger steering criterion, which has the ability to reveal the steering property of NOON states for all $N \geq 2$, which remains unable to be captured by any other previously derived steering criterion. We have also shown that the newly derived uncertainty relation has improved the lower bound on the secret key rate of a one-sided device independent quantum key distribution protocol for continuous variable systems [Chowdhury, Pramanik, and Majumdar, 2015] than that obtained in discrete variable systems.

In the last chapter, i.e., in Chapter-6, we have summarized the important results obtained in this thesis. We have also discussed about some future directions of study in this connection.