Quantum steering, entanglement and Bell nonlocality.

Frederick Denis Vas

October 16, 2014

Supervised by Professor Terence Rudolph

Submitted in partial fulfilment of the requirements for the degree of Master of Science of Imperial College London

Abstract

Quantum steering, the ability of one party to perform a measurement on their side of an entangled system with different outcomes leading to different sets of states for another part of the entangled system arbitrarily far away, is a purely quantum phenomena with no classical analogue. However, it is closely related (and indeed equivalent for pure states) to entanglement and Bell nonlocality.

This work reviews the connections between steering, entanglement and Bell nonlocality, and both the theoretical background and recent practical applications of steering.

Acknowledgements

This project would not have been possible without the help and support of many people.

Foremost, of course, was my dissertation supervisor, Professor Terence Rudolph, who patiently provided help and direction and with this work. I would also like to express my deep gratitude towards my Personal Tutor, Dr. Timothy Evans, and the MSc. Course director, Professor Kellogg Stelle, for their help throughout the year. The kindness shown by my boss, Daniel Rolles, in allowing me to take time off from work for this dissertation was also greatly appreciated.

A great debt is also owed to the Imperial administrative staff, both in the Physics Department and outside, whose unfailing and astonishingly cheerful help has made life so much easier. Finally, I am always grateful for the constant support shown by my friends and family, particularly during the last few months.

List of Abbreviations

Abbreviation	**Meaning**
CHSH inequality	Clauser-Horne-Shimony-Holt inequality
EPR paradox	Einstein-Podolsky-Rosen paradox
EPR-steering	Einstein-Podolsky-Rosen steering, quantum steering, steering
GHZ state	Greenberger-Horne-Zeilinger state
LHV models	Local Hidden Variable models
QKD	Quantum Key Distribution
DI-QKD	Device-Independent Quantum Key Distribution
1sDI-QKD	One-sided Device-Independent Quantum Key Distribution
QM	Quantum Mechanics
qubit	quantum bit

List of Symbols

Notation	Meaning
$\boldsymbol{C}$	The space of complex numbers, z
z	Complex number of the form $z = a + b\,i$
z^*	Complex conjugate of z, $z^* = a - b\,i$
A	Matrix of complex numbers
A^*	Complex conjugate of A
A^T	Transpose of A
$A^\dagger$	Hermitian conjugate of A, $A^\dagger = (A^T)^*$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}$
I	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Identity Matrix
X, σ_x	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Pauli Matrix
Y, σ_y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ Pauli Matrix
Z, σ_z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ Pauli Matrix
$\lvert\psi\rangle$	(*Ket*) State vector.
$\langle\psi\rvert$	(*Bra*) State vector, dual to $\lvert\psi\rangle$
$\langle\psi\rvert\psi\rangle$	Inner product of $\langle\psi\rvert$ and $\lvert\psi\rangle$
$\langle\psi\rvert A\lvert\psi\rangle$	Inner product of $\langle\psi\rvert$ and $A\lvert\psi\rangle$
$\lvert\psi\rangle \otimes \lvert\phi\rangle$	Tensor product of $\lvert\psi\rangle$ and $\lvert\phi\rangle$
$\lvert+\rangle$	$\frac{1}{\sqrt{2}}\,(\lvert0\rangle + \lvert1\rangle)$
$\lvert-\rangle$	$\frac{1}{\sqrt{2}}\,(\lvert0\rangle - \lvert1\rangle)$
$\lvert\beta_{00}\rangle$	$\frac{1}{\sqrt{2}}\,(\lvert00\rangle + \lvert11\rangle)$, Bell state
$\lvert\beta_{01}\rangle$	$\frac{1}{\sqrt{2}}\,(\lvert01\rangle + \lvert10\rangle)$, Bell state
$\lvert\beta_{10}\rangle$	$\frac{1}{\sqrt{2}}\,(\lvert00\rangle - \lvert11\rangle)$, Bell state
$\lvert\beta_{11}\rangle$	$\frac{1}{\sqrt{2}}\,(\lvert01\rangle - \lvert10\rangle)$, Bell state
$\lvert\psi_{GHZ}\rangle$	$\frac{1}{\sqrt{2}}\,(\lvert000\rangle + \lvert111\rangle)$, GHZ state

Contents

1 Introduction

Anyone who is not shocked by quantum theory has not understood it.

Niels Bohr

Quantum steering, a deeply disturbing idea from the viewpoint of classical physics, whereby one party can perform a measurement on their side of an entangled system with different outcomes leading to different sets of states for another part of the system that is arbitrarily far away, has been known of since the 1930s. However, it is only in the last 25 years that it was realised that for mixed states entanglement, steering, and Bell nonlocality were inequivalent. This realisation has led to increased interest in quantum steering, both for its own sake and because of its close links to entanglement and Bell nonlocality.

We begin by briefly reviewing the underlying mathematical ideas of the postulates of quantum theory. The concepts of entanglement and Bell nonlocality are covered in the following chapters before we turn our attention towards quantum steering. The final chapter deals with how quantum steering is related to entanglement and Bell non-locality for both pure and mixed states, and the recently discovered practical applications of quantum steering in the field of quantum key distribution.

1.1 Mathematical Preliminaries

The most incomprehensible thing about the world is that it is comprehensible.

Albert Einstein

In this section we briefly review the core mathematical elements of linear algebra needed to understand quantum mechanics. We begin with the definition of a complex vector space.

Definition
A complex vector space, V, is a set that is closed under both vector addition (denoted by +) and scalar multiplication (denoted by $\cdot$) and satisfies the following properties:

1. $\forall\ \overrightarrow{x}, \overrightarrow{y} \in V: \quad \overrightarrow{x} + \overrightarrow{y} \in V$
2. $\forall\ \overrightarrow{x}, \overrightarrow{y} \in V: \quad \overrightarrow{x} + \overrightarrow{y} = \overrightarrow{y} + \overrightarrow{x}$
3. $\forall\ \overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z} \in V: \quad (\overrightarrow{x} + \overrightarrow{y}) + \overrightarrow{z} = \overrightarrow{x} + (\overrightarrow{y} + \overrightarrow{z})$
4. $\exists\ \overrightarrow{0} \in V$ *such that* $\forall \overrightarrow{x} \in V,\ \overrightarrow{x} + \overrightarrow{0} = \overrightarrow{x}$
5. $\forall\ \overrightarrow{x} \in V\ \ \exists (-\overrightarrow{x})$ *such that* $\overrightarrow{x} + (-\overrightarrow{x}) = \overrightarrow{0}$

Scalar multiplication obeys:

1. $\forall\ \alpha \in \mathbf{C},\ \overrightarrow{x} \in V: \quad \alpha \overrightarrow{x} \in V$
2. $\forall\ x \in V: \quad 1 \cdot \overrightarrow{x} = \overrightarrow{x}$
3. $\forall\ \alpha, \beta \in \mathbf{C},\ \overrightarrow{x} \in V: \quad (\alpha \cdot \beta) \cdot \overrightarrow{x} = \alpha \cdot (\beta \cdot \overrightarrow{x})$
4. $\forall\ \alpha \in \mathbf{C},\ \overrightarrow{x}, \overrightarrow{y} \in V: \quad \alpha \cdot (\overrightarrow{x} + \overrightarrow{y}) = \alpha \cdot \overrightarrow{x} + \alpha \cdot \overrightarrow{y}$
5. $\forall\ \alpha, \beta \in \mathbf{C},\ \overrightarrow{x} \in V: \quad (\alpha + \beta) \cdot \overrightarrow{x} = \alpha \cdot \overrightarrow{x} + \beta \cdot \overrightarrow{x}$

Broadly speaking the underlying reason for representing quantum mechanics using a vector space framework is to remain consistent with the superposition principle.

Using this framework we can define the complex scalar product by

Definition
A complex scalar product on a vector space space is a function that assigns to every set of two vectors $\overrightarrow{x}, \overrightarrow{y} \in V$ a complex number $(\overrightarrow{x}, \overrightarrow{y})$ satisfying:

1. $\forall\ \overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z} \in V,\ \ \alpha, \beta \in \mathbf{C}: \quad (\overrightarrow{x}, \alpha \overrightarrow{y} + \beta \overrightarrow{z}) = \alpha(\overrightarrow{x}, \overrightarrow{y}) + \beta(\overrightarrow{x}, \overrightarrow{z})$
2. $\forall\ \overrightarrow{x}, \overrightarrow{y} \in V: \quad (\overrightarrow{x}, \overrightarrow{y}) = (\overrightarrow{y}, \overrightarrow{x})^*$
3. $\forall\ \overrightarrow{x} \in V: \quad (\overrightarrow{x}, \overrightarrow{x}) \geq 0$
4. $\forall\ \overrightarrow{x} \in V: \quad (\overrightarrow{x}, \overrightarrow{x}) = 0 \Leftrightarrow \overrightarrow{x} = 0$

Complex vector spaces which have been assigned a scalar product are known as unitary vector spaces. We can now use the scalar product to define the norm ('length') of a vector and the concept of orthogonal vectors.

Definition
The norm of a vector $\overrightarrow{x} \in V$ *is given by* $||\overrightarrow{x}|| = \sqrt{(\overrightarrow{x}, \overrightarrow{x})}$.

Definition
The vectors $\overrightarrow{x}, \overrightarrow{y} \in V$ *are said to be orthogonal if* $(\overrightarrow{x}, \overrightarrow{y}) = 0$.

Finally we can now define Hilbert spaces for the final dimensional cases we are primarily concerned with:

Definition
A complex vector space, $\mathcal{H}$*, is a Hilbert space if:*

1. $\mathcal{H}$ *is an unitary vector space.*
2. $\mathcal{H}$ *is complete.*

Completeness here refers to a property of a vector space whereby the limit of any convergent (Cauchy) sequence of elements from the vector space is itself a member of the vector space.

We can now understand why the Hilbert space is the mathematical structure used to represent quantum mechanics. First, it is a vector space, and so is consistent with the superposition principle. Second it is a complete vector space so the limit of any convergent sequence of physical states will also be a physical state in the Hilbert space, as our physical intuition would suggest.

Having very briefly outlined the mathematical foundations we now turn our attention to the fundamental postulates of quantum mechanics.

1.2 The Postulates of Quantum Mechanics

> *If we look at the way the universe behaves, quantum mechanics gives us fundamental, unavoidable indeterminacy, so that alternative histories of the universe can be assigned probability.*
>
> Murray Gell-Mann

We now consider the postulates of quantum mechanics[1], and their significance. The first postulate describes the mathematical structure we use to represent quantum mechanical systems.

Postulate 1:
Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, $|\psi\rangle$, which is a unit vector in the system's state space.

As mentioned before, Hilbert space is a natural mathematical choice as it is consistent with both the superposition principle and our physical intuition that the limit of any convergent sequence of physical states should also be a physical state.

The definition leaves open the question of what the state space and state vector of the system is for any given physical system. In this work, the systems we will be primarily concerned with are simply the quantum bit (or qubit) and its generalisations.

The second postulate deals with the issue of how a quantum mechanical state, $|\psi\rangle$, evolves with time.

Postulate 2:
The evolution of a closed quantum system is described by a unitary transformation. That is, the state of the system at time t_1 is related to the state of the system at time t_2 by a unitary operator, U, which depends only on the times t_1 and t_2:

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

[1]These are quoted almost *verbatim* from Nielsen and Chuang's textbook on 'Quantum Computation and Quantum Information' [1].

Here an unitary operator, U, is defined as an operator satisfying the condition $U^\dagger U = UU^\dagger = I$ where I being the identity matrix.

This postulate is, of course, an idealisation as apart for the entire Universe there is no such thing as a truly closed system. From an experimental point of view we can we can consider a closed system as one for which any outside influences are negligible. Given our subject matter is somewhat ironic, as one of the major issues in practical applications such as quantum computing is being able to interact with the system enough to precisely control it while at the same time making it resilient to unwanted outside influences.

Another idealisation inherent in this postulate is that it only deals with the quantum state of a system at two different times. Consequently for continuous time systems we have

Postulate 2a:
The (continuous) time evolution of the state of a closed quantum system is described by the Schrödinger equation,

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where $\hbar$ is a physical constant known as Planck's constant, and H is a fixed Hermitian (i.e. obeying $H = H^\dagger$) operator known as the Hamiltonian of the closed system.

Having postulated the time evolution of a quantum system we now consider how to describe what happens when we actually interact with it. This is covered by:

Postulate 3:
Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I$$

The intuitive justification behind this postulate is that if we measure a quantum system twice with the second measurement being immediately after the first we would expect to obtain the same result. Moreover the completeness equation ensures that the probability of the various outcomes sum to one. Interestingly, as was proved by Andrew Gleason [2] in 1957, it turns out that the the choice of the probability measure is essentially unique given the Hilbert space structure of quantum mechanics.

However, the fundamental issue of when exactly the reduction of the quantum mechanical state (or 'wavefunction') takes place has always been a contentious issue, despite the fact that the postulate describes the result of experiments very well. Consequently taking our cue from Richard Feynman's quip that, *the 'paradox' is only a conflict between reality and your feeling of what reality 'ought to be'* we now move on to the final postulate that describes a composite quantum system made up of two or more physical systems.

Postulate 4:
The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 *through* n*, and system number* i *is prepared in the state* $|\psi_i\rangle$*, then the joint state of the total system is* $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$*.*

where the symbol $\otimes$ denotes the tensor product. From this we see if we have a particle A with state $|\psi_A\rangle$ in Hilbert space $\mathcal{H}_A$ and particle B with state $|\phi_B\rangle$ in Hilbert space $\mathcal{H}_B$ then the total state of the two-particle system can be written as $|\psi_A\rangle \otimes |\phi_B\rangle$, or even more succinctly as $|\psi_A\rangle|\phi_B\rangle$, in the Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ of the combined system.

This definition also very naturally leads on to the idea of product and entangled states which we will cover in the next chapter.

1.3 The Path Ahead

Having briefly reviewed the postulates of quantum theory and the underlying mathematics, we now look at the ideas of entanglement, Bell nonlocality and quantum steering, and their fascinating inter-relationships.

2 Entanglement

> *Isolated material particles are abstractions, their properties being definable and observable only through their interaction with other systems.*
>
> Niels Bohr

Quantum entanglement is the term given to the phenomena whereby particles can be generated or interact in ways such that the quantum state of each particle cannot be described independently. In such cases the system of particles is said to be entangled and it is not correct to consider any of the individual particles in isolation from the others, but only as a single, entangled state.

The concept of entanglement is usually traced back to the famous 1935 paper [3] by Albert Einstein, Boris Podolsky and Nathan Rosen where they presented what is now known as the EPR (Einstein-Podolsky-Rosen) paradox, which attempted to show that quantum mechanics was incomplete. Indeed Einstein later famously derided the idea of entanglement as "*spukhafte Fernwirkung*" or "*spooky action at a distance*" as it seemed to violate the local realist view of causality contrary to the spirit of his theory of relativity.

However as Hrvoje Nikolić pointed out in his 2012 paper on 'EPR before EPR: a 1930 Einstein-Bohr thought experiment revisited' [4], Einstein had unknowingly stumbled across an equivalent problem in 1930 when he had argued against consistency of the energy-time uncertainty relation with a thought experiment involving a measurement of the mass of a box that had emitted a photon. Even earlier, at the 1927 Solvay conference, Einstein's presentation focused on problems of interpretation associated with the collapse of the wave function in a thought experiment during which electrons pass through a small hole and were then uniformly dispersed in the direction of a hemispherical photographic film-screen surrounding the hole. Einstein mused that "*the interpretation, according to which* $|\psi|^2$ *expresses the probability that this particle is found at a given point, assumes an entirely peculiar mechanism of action at a distance, which prevents the wave continuously distributed in space from producing an action in two places on the screen.*"

Nonetheless it was Erwin Schrödinger who in a letter to Einstein about the issues raised by EPR, first used the word "*Verschränkung*", that he later translated as "*entanglement*", to "*describe the correlations between two particles that interact and then separate, as in the EPR experiment*". Shortly thereafter, in a paper [5] where Schrödinger defined and discussed the notion of entanglement he stated, "*I would not call [entanglement] one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought*". Schrödinger also considered the possibility that resolution of the EPR paradox might lie in quantum mechanics breaking down for distant entangled systems via what is nowadays known as quantum decoherence. However, this is now known not to be the case.

Despite these reservations by two of the people most intimately involved with its genesis, entanglement has nevertheless been experimentally confirmed many times since their seminal papers including in photons, electrons, small molecules [6], and recently even millimeter-sized diamonds [7].

We will continue the discussion about the EPR paradox in the following chapter. For now, we investigate in detail the consequences of entanglement, beginning with a discussion of entangled quantum bits.

2.1 Quantum Bits

Quantum bits (or qubits as they are frequently referred to) are a generalization of the classical bit. Classically, information can be represented in the form of bits denoted by the logical values of 0 and 1 which can be thought of as representing, for example, a uncharged and charged transistor respectively. As such macroscopic objects contain a huge number of elections this description is satisfactory as the difference in the number of electrons in a charged or uncharged transistor is very clear.

However, as we begin to deal with smaller and smaller systems, and especially as we near the atomic level, the applicable laws become that of quantum mechanics. In this scenario, not only is the system far more sensitive to outside perturbations, but we are also forced to take into account the superposition principle. Consequently, a quantum bit is represented in the form

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

which $|\psi\rangle$ is usually taken to be normalized so that $\langle\psi|\psi\rangle = 1$, or equivalently that $|a|^2 + |b|^2 = 1$.

This has the distinctly non-classical feature that we can simultaneous represent two values using just a single bit. Similarly, we find that a system of two qubits can be in a coherent superposition of four different states:

$$|\psi\rangle = a|0\rangle|0\rangle + b|0\rangle|1\rangle + c|1\rangle|0\rangle + d|1\rangle|1\rangle$$

and that a n qubit system can be in a coherent superposition of 2^n quantum states.

Consequently by applying an unitary transformation to a n-qubit system we can potentially manipulate 2^n numbers simultaneously. This represents a massive potential parallelism gain for our computational abilities, allowing quantum computers to solve certain problems exponentially faster than their classical rivals. Sadly, although perhaps not that unexpectedly, it is proving to be very difficult to build a quantum system so that we can control its state very precisely while at the same time making it robust against the effects of noise. A very comprehensive review of this subject can be found in the textbook by Nielsen and Chaung [1], with an up-to-date timeline for the development of quantum computing at [8]. For our part, however, we must leave this fascinating topic to consider another consequence of the superposition principle of quantum mechanics in the next section.

2.2 Entanglement and Product States

The idea of entanglement was first explicitly mentioned by Erwin Schrödinger in a letter to Einstein about the issues raised by the EPR paper, and is perhaps best known with regard to his famous thought experiment involving an unfortunate (yet also simultaneously not) cat which Schrödinger describes [9] as follows;

> *One can even set up quite ridiculous cases. A cat is penned up in a steel chamber, along with the following device (which must be secured against direct interference by the cat): in a Geiger counter, there is a tiny bit of radioactive substance, so small, that perhaps in the course of the hour one of the atoms decays, but also, with equal probability, perhaps none; if it happens, the*

> *counter tube discharges and through a relay releases a hammer that shatters a small flask of hydrocyanic acid. If one has left this entire system to itself for an hour, one would say that the cat still lives if meanwhile no atom has decayed. The psi-function of the entire system would express this by having in it the living and dead cat (pardon the expression) mixed or smeared out in equal parts.*
>
> ...
>
> *It is typical of these cases that an indeterminacy originally restricted to the atomic domain becomes transformed into macroscopic indeterminacy, which can then be resolved by direct observation. That prevents us from so naively accepting as valid a"blurred model" for representing reality. In itself, it would not embody anything unclear or contradictory. There is a difference between a shaky or out-of-focus photograph and a snapshot of clouds and fog banks.*

This thought experiment deals with the extremely thorny issue of when the translations occur between a quantum system existing as a superposition of states and a classical system with (at least in the ideal world of Laplace) an unique and completely knowable state. Without delving into the metaphysical and philosophical arguments raised by this thought experiment, this argument nonetheless makes it very clear that there are distinctly non-classical features involved with quantum states.

Mathematically speaking, we see that entanglement arises from the combination of the superposition principle and the tensor product structure of the Hilbert space for quantum mechanics. We can best understand this idea by means of an example. Consider the following state of a two particle system:

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

States such as this are known as product, separable or disentangled states since the result of a measurement on the first system is completely independent of the result of a measurement on the second system.

However, states such as

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

are called entangled or non-separable states since if we measure $|0\rangle$ for the first system we know that the second system must also be in state $|0\rangle$, while if our measurement for the first system is $|1\rangle$ we know that the second system must be also be in state $|1\rangle$.

Up to this point there is nothing that is not reproducible in a classical setting. For example we can produce the same correlations classically using a system with two coins that is prepared in such a way that both always show either heads or tails. The fundamental difference, however, lies in the fact that for quantum mechanical systems we can measure in a basis other than $\{|0\rangle,|1\rangle\}$ such as $\{|+\rangle, |-\rangle\}$ defined by $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The importance of this difference will be apparent when we consider the EPR nonlocality paradox later on.

Determining how entangled a particular state is can be extremely complicated, and to do this we first need to introduce the concepts of a density operator and pure and mixed states. The density operator, ρ describes a quantum system that is in one of a number of states $|\psi_i\rangle$ with probability p_i, so that

$$|\psi\rangle = \sum_i p_i |\psi_i\rangle$$

The density operator is then given by

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

If we know the exact state of a quantum system then it is known as a pure state, and the density operator is $\rho = |\psi_i\rangle\langle\psi_i|$. Otherwise the quantum system is said to be in a mixed state. A simple criterion for differentiating between them is given by taking the trace of the square of the density matrix, $Tr(\rho^2)$. For a pure state this will always be one while a mixed state will have a value of less than one.

We can now define a common measure for pure states called the entanglement entropy that is given by the the von Neumann entropy of the reduced density operator of the state. For a pure state $\rho_{AB} = |\psi\rangle\langle\psi|$ this is:

$$\mathcal{E}(\rho_{AB}) = \mathcal{S}(\rho_A) = \mathcal{S}(\rho_B)$$

where Tr denotes the trace for $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B = \mathrm{Tr}_A(\rho_{AB})$, and $\mathcal{S}$ is the von Neumann entropy defined by:

$$\mathcal{S} = -\mathrm{Tr}(\rho \ln \rho)$$

where ρ is the density matrix of the quantum mechanical system.

In two dimensions a specific set of maximally entangled quantum states are given by the Bell states:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle + |10\rangle\right)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle - |11\rangle\right)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle\right)$$

while for three dimensions a natural candidate is the Greenberger-Horne-Zeilinger (GHZ) state:

$$|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle\right)$$

2.3 Superdense Coding

A striking example of the fundamental difference between classical and quantum systems is provided by superdense coding. Suppose we have two parties, who in deference to convention we name Alice and Bob. Alice wishes to transmit two bits of classical information to Bob but can only send one qubit. Since non-orthogonal quantum states cannot be reliably distinguished, it would appear that this should not be possible, and indeed just as for the classical case we find that only one classical bit of information can be transmitted. However, if Alice and Bob are allowed to also share a maximally entangled state it turns out that two classical bits of information per qubit can be transmitted thus giving rise to the term superdense coding.

We assume that Alice and Bob initially share a pair of qubits in the maximally entangled state

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

that could have been sent to Alice and Bob by a third party far in advance. Here, for clarity, the first qubit is denoted with an A and the second with a B to emphasise that they are held by Alice and Bob respectively.

Alice can now communicate two bits of classical information to Bob by sending him the single (unentangled) qubit in her possession:

To send the bit string '00' to Bob she simply sends her qubit as it is.

To send '01' she performs the $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ Pauli matrix operation on her qubit before sending it.

To send '10' she performs the $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Pauli matrix operation on her qubit before sending it.

Finally, if she wants to send '11' she performs the $iY = i \cdot \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ Pauli matrix operation on her qubit before sending it.

The resulting state of her qubit is then given by a Bell state:

Bit String	Final state of B's qubit.
00	$\frac{1}{\sqrt{2}} \left(\|00\rangle + \|11\rangle\right)$
01	$\frac{1}{\sqrt{2}} \left(\|00\rangle - \|11\rangle\right)$
10	$\frac{1}{\sqrt{2}} \left(\|01\rangle + \|10\rangle\right)$
11	$\frac{1}{\sqrt{2}} \left(\|01\rangle - \|10\rangle\right)$

which since the Bell states form an orthonormal basis can be unambiguously distinguished by an appropriate quantum measurement. Consequently Bob upon receiving Alice's qubit can by performing a measurement in the Bell basis determine which of the four bit strings Alice had sent. Interestingly it also turns out that the two classical bits of information that we have seen it is possible to send using this method is actually the maximum amount of classical information that can be sent in this fashion.

3 Bell Nonlocality

God does not play dice with the universe.

Albert Einstein

If the price of avoiding non-locality is to make an intuitive explanation impossible, one has to ask whether the cost is too great.

David Bohm

After the intentionally ironic quote by Einstein, who despite contributing to the creation of quantum mechanics by his work on the photo-electric effect even to his dying day never truly accepted it, we now consider the ideas underlying Bell non-locality. These ideas can, as was the case for entanglement, be traced back to the 1935 paper [3] by Albert Einstein and his postdoctoral research associates Boris Podolsky and Nathan Rosen. However, unlike entanglement, a proper appreciation of the concept of Bell non-locality requires it to be placed in the appropriate historical context, which we now set out to do.

The Heisenberg uncertainty principle, a cornerstone of quantum mechanics, states that there is a fundamental limit to the precision to which the physical properties of certain pairs of complementary variables, such as position and momentum, can be simultaneously known. In addition, the standard Copenhagen interpretation of quantum mechanics takes literally the quote by Ludwig Wittgenstein that "*Whereof One Cannot Speak, Thereof One Must Be Silent*", so that it is only when we measure a value of a property of a particle that the property gains physical reality whilst before the measurement the particle must be considered to be in a superposition state. Finally, quantum mechanics allows a description by a single wave function of an entangled pair of quantum systems that encodes the probabilities of the outcomes of individual or joint experiments performed on the two sub-systems.

The crux of the the EPR paper lies in the fact that if we consider two such entangled particles, A and B, then in quantum mechanics measuring a certain property of particle A can cause the complimentary property of particle B to become uncertain, even if there was no possible classical interaction between them. Of course, in classical physics there is no such paradox since it is implicitly assumed that all the properties of a particles have a

definite value at all times, and the act of measurement only reveals these pre-existing values. However, in quantum mechanics this is not the case.

To make their argument EPR gave an operational definition of an '*element of reality*'[2] :

> *If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.*

Consequently, if a physical property of an object can be definitely known without it being observed, then to agree with this definition of physical reality, the property cannot have been created by the observation and must have possessed a prior physical reality.

EPR also took for granted the principle of locality, namely that a physical processes occurring at one location cannot have an instantaneous effect on elements of reality at another location. This appeared to them to be a natural consequence of special relativity in which information transmission faster than the speed of light would lead to causality violation, and the consequential paradoxes.

For such locally realistic theories[3], EPR considered what would happen to two particles, A and B, which interacted briefly and then moved off in opposite directions. As it is possible to measure arbitrarily accurately the exact position of particle A, then by calculation we can also know with certainty the exact position of particle B. However, it would equally be possible to measure the exact momentum of particle A and so determine the exact momentum of particle B.

Consequently EPR argued that, using their definition of realism, particle B must have definite values for both position and momentum simultaneously, contrary to what was expected from quantum mechanics. EPR considered

[2] Nowadays EPR's definition of reality has been somewhat superseded by the idea of counterfactual definiteness, namely that outcomes of measurements that were not actually performed are viewed as being just as much part of reality as those that were actually made.

[3] Also implicit is the freedom-of-choice principle, which concerns the independence of the choice of measurements and the internal state of the physical system being measured. This is not covered in any detail here as while certain variants of this principle can be experimentally tested, it is hard to see how it could ever be possible to rule out all versions of this principle.

two possible explanations for this contradiction. The first was that there could be an interaction between the particles even though they were separated. This would, however, seem to contradict the spirit of relativity. The second was that the information about the outcome of all possible measurements was already present in both particles which is at variance with the quantum mechanical interpretation. As EPR took for granted the principle of locality they therefore concluded that '*the quantum-mechanical description of physical reality given by wave functions is not complete*". By this they meant that quantum mechanics is actually an incomplete theory and that there was a still deeper theory of nature of which quantum mechanics is merely a statistical approximation. Such a deeper theory would contain variables corresponding to all the '*elements of reality*' and is referred to as a hidden variable theory.

The EPR paper generated a great deal of interest, not to mention controversy, about the foundations of quantum mechanics and hidden variable models. However, it still took almost 30 years for the pivotal breakthrough in this field to take place, and it was only in 1964 that John Bell proved [10], as we shall see in the following section, that EPR's key assumption of locality was not consistent with a hidden variables interpretation of quantum theory.

3.1 Bell's Theorem

What is proved, by impossibility proofs, is lack of imagination.

John Bell

Bells theorem is the most profound discovery of science.

Henry P. Stapp

Bell's theorem is is the collective name for a family of results that draw a clear distinction between quantum mechanics and local hidden variable theories. It was originally[4] proved by the eponymous John Bell in his 1964 paper [10], building on earlier work by David Bohm [11], who in turn had investigated the issues raised by Einstein, Podolsky and Rosen in their 1935 paper [3]. By considering spin measurements on pairs of entangled electrons Bell managed to derive a testable inequality that all local hidden variable theories must obey. Equally importantly, he also gave specific cases where these prediction were different to that of quantum mechanics, thereby making it possible to determine experimentally what actually occurs in nature.

We now provide one of the most straightforward derivations of Bell's Theorem, following very closely the proof given in [12].

We begin by considering the state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)$$

when it used to describe a system of two spin-$\frac{1}{2}$ particles in a local hidden variable theory. We measure the orientation of the spin of the first particle along direction $\overrightarrow{a}$, and the orientation of the spin of the second particle along direction $\overrightarrow{b}$, with each measurement having only two outcomes, either parallel or anti-parallel. If the result of the measurement for the first particle is parallel we take the value of a to be one and if anti-parallel we set a to minus one, and similarly for the second particle with the variable b. By repeating this experiment N times we can then define the correlation between the two measurements by:

[4]While the mathematician von Neumann had presented a proof in 1932 that hidden variable theories of the type later considered by EPR were impossible he had made an incorrect assumption, leaving the issue still unresolved.

$$C(\overrightarrow{a},\overrightarrow{b}) = \lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} a_n b_n$$

Our assumption that the theories under consideration are locally realistic has two main consequences. First locality ensures that a measurement on the first particle can have no effect on the measurement of the second particle if they are space-like separated so there is no time for light to travel from the particle measured first to the other particle before that is measured. This means that the joint probabilities being considered will simply reduce to the probability of the outcome for the first particle multiplied by the probability of the outcome for the second particle. Second, the hidden variables influence the probabilities we measure, so that all such probabilities can be written in the form $P_A(a,\lambda)$ or $P_A(b,\lambda)$, where λ represents the hidden variables.

Under these assumptions we find that measurements along the four directions $\overrightarrow{a}$, $\overrightarrow{a'}$, $\overrightarrow{b}$ and $\overrightarrow{b'}$ obey the Bell[5] inequality

$$|C(\overrightarrow{a},\overrightarrow{b}) + C(\overrightarrow{a},\overrightarrow{b'}) + C(\overrightarrow{a'},\overrightarrow{b}) - C(\overrightarrow{a'},\overrightarrow{b'})| \leq 2 \qquad (1)$$

We can see this by writing

$$\begin{aligned} C(\overrightarrow{a},\overrightarrow{b}) &= \int d\lambda\ \rho(\lambda)\ [P_A(1,\lambda)P_B(1,\lambda) + P_A(-1,\lambda)P_B(-1,\lambda) \\ &\qquad -P_A(1,\lambda)P_B(-1,\lambda) - P_A(-1,\lambda)P_B(1,\lambda)] \\ &= \int d\lambda\ \rho(\lambda)\ [P_A(1,\lambda) - P_A(-1,\lambda)]\ [P_B(1,\lambda) - P_B(-1,\lambda)] \\ &\equiv \int d\lambda\ \rho(\lambda)\ Q_A(\overrightarrow{a},\lambda)\ Q_B(\overrightarrow{b},\lambda) \end{aligned}$$

and by using the fact that

$$|a_n(b_n + b_n') + a_n'(b_n - b_n')| \leq 2$$

for all $\overrightarrow{a}, \overrightarrow{a'}, \overrightarrow{b}, \overrightarrow{b'} \in [-1,1]$ we find that, as required

[5]This is also known as the CHSH inequality [13] after the initials of its four discoverers: John Clauser, Michael Horne, Abner Shimony and Richard Holt.

$$
\begin{aligned}
& |C(\overrightarrow{a}, \overrightarrow{b}) + C(\overrightarrow{a}, \overrightarrow{b'}) + C(\overrightarrow{a'}, \overrightarrow{b}) - C(\overrightarrow{a'}, \overrightarrow{b'})| \\
\leq & \int d\lambda \ \rho(\lambda) \ [Q_A(\overrightarrow{a}, \lambda)\, Q_B(\overrightarrow{b}, \lambda) + Q_A(\overrightarrow{a}, \lambda)\, Q_B(\overrightarrow{b'}, \lambda) \\
& \qquad + Q_A(\overrightarrow{a'}, \lambda)\, Q_B(\overrightarrow{b}, \lambda) - Q_A(\overrightarrow{a'}, \lambda)\, Q_B(\overrightarrow{b'}, \lambda)] \\
\leq & \ 2
\end{aligned}
$$

By comparison in quantum mechanics the correlation value is given by

$$C(\overrightarrow{a}, \overrightarrow{b}) = \langle\psi|(\overrightarrow{a}\,\hat{\overrightarrow{\sigma}}) \otimes (\overrightarrow{a}\,\hat{\overrightarrow{\sigma}})|\psi\rangle$$

where $\hat{\overrightarrow{\sigma}} = \hat{\overrightarrow{\sigma_x}}\overrightarrow{e_x} + \hat{\overrightarrow{\sigma_y}}\overrightarrow{e_y} + \hat{\overrightarrow{\sigma_z}}\overrightarrow{e_z}$ for Pauli operators $\hat{\overrightarrow{\sigma_i}}$, which we can rewrite in terms of the angle θ_{ab} between the vectors $\overrightarrow{a}$ and $\overrightarrow{b}$ as

$$C(\overrightarrow{a}, \overrightarrow{b}) = -\cos\theta_{ab}$$

We now choose the vectors $\overrightarrow{a}$, $\overrightarrow{a'}$, $\overrightarrow{b}$ and $\overrightarrow{b'}$ to be all coplanar, with $\overrightarrow{a}$ and $\overrightarrow{b}$ parallel and facing in the same direction, while $\overrightarrow{a'}$ and $\overrightarrow{b'}$ lie at the same angle ψ, but on opposite sides of $\overrightarrow{a}$ and $\overrightarrow{b}$. Inserting these values into Bell's inequality, equation [1] becomes:

$$|1 + 2\cos\theta - \cos 2\theta| \leq 2$$

which is found to be violated for certain values of θ, with a maximum value of 2.5 occurring for $\theta = \pi/3$. This result marked a historic breakthrough as it meant that experiments could finally be used to determine whether quantum mechanics or a hidden variable model was the correct description of nature.

However, it turned out that such experimental tests were quite difficult in the case of electrons as Bell had originally considered, but it was found that entangled photons also obeyed similar Bell inequalities and were easier to work with. Such experiments were carried out by John Clauser and Stuart Freedman [14] in 1972, and Alain Aspect, Philippe Grangier, and Gérard Rogeret [15] in 1981, and are generally believed to rule out hidden variable theories in favour of quantum mechanics.

Unfortunately, although the outcome of every single experiment so far carried out has been in favour of quantum mechanics as opposed to locally realistic theories, it has not been possible to simultaneously close three potential loopholes. The first of these is the locality, or communication, loophole

which requires that there be no causal way for a measurement of one particle to affect the other. To avoid this the experimenter must ensure that the particles have travelled far enough apart before being measured, and that the measurement process is also rapid enough, that light does not have time to travel between the start of either detection and the finish of the other. The second loophole is the detection, or unfair sampling, loophole which deals with the fact that only a certain percentage of the photons are detected. With a less than perfect detection rate the value of the right-hand side of the CHSH inequality

$$|C(\overrightarrow{a}, \overrightarrow{b}) + C(\overrightarrow{a}, \overrightarrow{b'}) + C(\overrightarrow{a'}, \overrightarrow{b}) - C(\overrightarrow{a'}, \overrightarrow{b'})| \leq 2$$

is increased and below $2(\sqrt{2} - 1) \equiv 83\%$ efficiency it is not possible to say with certainty that the violation is due to quantum mechanics being correct as opposed to detection inefficiency. As optical tests of Bell's theorem tend to have relatively low efficiencies this poses a serious potential issue. The final loophole is the freedom-of-choice loophole, which deals with possibility that the source of the entangled particles can somehow communicate classically with the detectors and thereby affect the measurements being made.

Despite these obstacles, there has been notable recent advances in this area. In 2001 Rowe et al. [16] by using Be^+ ions rather than photons achieved a high enough efficiency to close the detection loophole. This was followed in 2010 by a team led by Anton Zeilinger managing to close both the locality and the freedom-of-choice loophole simultaneously for photons, and the same group [17] last year also managing to close the detection assumption for photons (although not simultaneously with the other loopholes). Finally this year, Erven et al. [18] demonstrated three-party quantum nonlocality using a three-photon entangled GHZ state whilst simultaneously closing both the locality and freedom-of-choice loopholes.

Nonetheless while no loophole-free Bell test has yet been performed, the vast majority of scientists regard the current evidence as being overwhelmingly in favour of quantum mechanics and against local hidden variable theories. Consequently it would appear that one of the classical concepts of locality or realism (or perhaps even freedom-of-choice) is untenable. Having described the theoretical and experimental work that lead to this startling conclusion, we now consider a practical application of Bell states.

3.2 Quantum Teleportation

Quantum teleportation, or quantum state teleportation, as it might be more appropriately be described is the process by which the exact quantum state of a particle can be transmitted from one location to another. This idea might seem at first sight to be paradoxical given the uncertainty principle in quantum mechanics since we cannot determine the precise state of an arbitrary quantum system. However, the existence of entangled states enables us to conduct the teleportation protocol without ever needing to determine the exact state of the test system.

We now describe quantum teleportation[6] in the form proposed by the seminal paper [19] by Bennett et al. published in 1993. Our two observers Alice and Bob are currently distant from each other, but share a maximally mixed Bell state

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

where, as before, the first qubit is denoted with an A and the second with a B to emphasise that they are held by Alice and Bob respectively. Alice also holds a qubit whose exact state is unknown to her,

$$|\phi\rangle = a|0\rangle| + b|1\rangle$$

that she wishes to teleport to Bob.

Note that if Alice knew the exact state of her state she could simply pass this information classically to Bob who could then replicate it without needing to use their shared entangled state. However even in this case, given that one can sometimes need an infinite amount of classical information to precisely describe the state of a system, quantum teleportation would still retain certain theoretical advantages.

The combined state of the three qubit system can be written as:

$$|\phi_{AB}\rangle = |\phi\rangle|\psi_{AB}\rangle = \frac{1}{\sqrt{2}} \left(a|0\rangle| + b|1\rangle\right) \left(|00\rangle + |11\rangle\right)$$

which we can rewrite in the Bell state basis as

[6] It seems more appropriate to discuss this topic here, rather than in the chapter on entanglement as the nature of quantum teleportation raises the issue of nonlocality.

$$
\begin{aligned}
|\phi_{AB}\rangle &= \frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right) \\
&= \frac{1}{2}[\quad |\beta_{00}\rangle(a|0\rangle + b|1\rangle) + |\beta_{10}\rangle(a|0\rangle - b|1\rangle) \\
&\qquad + |\beta_{01}\rangle(a|1\rangle + b|0\rangle) + |\beta_{11}\rangle(a|1\rangle - b|0\rangle)\ ]
\end{aligned}
$$

where $|\beta_{00}\rangle$, $|\beta_{01}\rangle$, $|\beta_{10}\rangle$ and $|\beta_{11}\rangle$ are the maximally entangled quantum Bell states given by:

$$
\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)
\end{aligned}
$$

The teleportation protocol is now implemented by Alice performing projective measurements using the Bell basis on the two qubits she holds. She will then obtain one of the four Bell states with equal probability. If she obtains, say $|\beta_{01}\rangle$, then the combined state of all three qubits has been collapsed to

$$
|\beta_{01}\rangle_A\ (a|1\rangle_B + b|0\rangle_B)
$$

and she must now classically communicate that she has obtained the Bell state $|\beta_{01}\rangle$ to Bob.

After Bob receives this information he can complete the teleportation procedure by performing the unitary $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Pauli matrix operation on his qubit thereby obtaining the state $a|0\rangle + b|1\rangle$ which is identical to the one that Alice originally held.

Similarly if Alice had found the state of her two qubits to have been $|\beta_{00}\rangle$, $|\beta_{10}\rangle$ or $|\beta_{11}\rangle$ then by performing the unitary $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $iY = i \cdot \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ operation on his qubit Bob can again obtain the state $a|0\rangle + b|1\rangle$.

As all the operations carried out have been local in nature this implies that the above protocol does in fact correspond to a proper quantum teleportation of the unknown state from Alice to Bob.

It is however important to realise that this process cannot be used for superluminal communication since a vital requirement is that Alice must transmit her measurement result to Bob using classical communication, and that this communication is limited to the speed of light. In fact it can be shown (see section 2.4.3 of [1]) that without this classical communication, the use of quantum teleportation conveys no information gain whatsoever.

Quantum teleportation also cannot be used to make copies of a system, since after the process is complete the original state of the particle held by Alice has been erased. This is an example of the no-cloning theorem in quantum mechanics that forbids the creation of identical copies of an arbitrary, unknown quantum state [20].

Nonetheless, ever since its inception the field of quantum teleportation has attracted a great deal of interest. Recent experimental advances include one research group managing to achieve quantum teleportation of photons over a distance of 143 kilometers [21] and another group announcing a reliable method of transferring data by quantum teleportation [22].

4 Quantum Steering

> *It is rather discomforting that the theory should allow a system to be steered or piloted into one or the other type of state at the experimenter's mercy in spite of his having no access to it.*
>
> Erwin Schrödinger

Quantum steering (which is also referred to in the literature as EPR-steering or simply steering) is a deeply disturbing idea from the viewpoint of classical physics whereby one party can perform a measurement on their side of an entangled system with different outcomes leading to different sets of states for another system arbitrarily far away.

The concept of steering had its origin in the 1935 EPR paper [3] where Einstein and his collaborators considered the general unfactorisable pure state of two systems:

$$|\Psi\rangle = \sum_{n=1}^{\infty} c_n |u_n\rangle|\psi_n\rangle = \sum_{n=1}^{\infty} d_n |v_n\rangle|\phi_n\rangle \tag{2}$$

where $\{|u_n\rangle\}$ and $\{|v_n\rangle\}$ are two different orthonormal basis for the first system. By identifying the first set of basis as belonging to Alice and the second to Bob, we can see that if Alice were to measure in the $\{|u_n\rangle\}$ basis she would, according to quantum mechanics, instantaneously cause Bob's system to collapse into one the $|\psi_n\rangle$ states. Alternatively if Alice instead measured in the $\{|v_n\rangle\}$ basis, quantum mechanics implies that Bob's system would instantaneously collapse into one of the $|\phi_n\rangle$ states.

The fact that $\{|\psi_n\rangle\}$ is different to $\{|\phi_n\rangle\}$ was problematic to EPR as the two systems could be widely separated and they therefore felt that no real change could take place. In his reply to the EPR paper, Schrödinger introduced the terms 'entangled' to describe states such as (2), and 'steering' to describe the ability of Alice to affect Bob's state by her choice of measurement basis. Soon thereafter he also proved [5] the quantum steering theorem[7], for linearly independent, although possibly non-orthogonal, ensembles of states:

[7]Note that we use the version given in [23].

Theorem
Given an entangled state $|\psi_{AB}\rangle$ of two systems A and B, then a measurement on system A can collapse system B to the set of states $\{|\phi_i\rangle\}$ with associated probabilities p_i if and only if

$$\rho_B = \sum_i p_i |\phi_i\rangle\langle\phi_i|$$

where $\rho_B \equiv Tr_A|\psi_{AB}\rangle\langle\psi_{AB}|$ is the reduced state of system B.

However, despite this proof and the conceptual issues raised by EPR, the concept of steering (and steerable states) seems to have quietly slipped into obscurity. The probable reason for this is that for the pure states that were generally considered at the time the concepts of entanglement, steering and Bell nonlocality coincide. This seems to have been implicity appreciated by physicists of the time although never outright stated. Consequently, they were more than happy to simply deal the more clearly defined concepts of entanglement and Bell nonlocality.

It was not until 1989 that Werner [24] investigated the relationship between entanglement and Bell-nonlocality for mixed states and discovered that not all entangled states were Bell nonlocal. This naturally raised the issue of what the exact relationship for mixed states was between steering, entanglement and Bell nonlocality. This was answered in two papers [25],[26] by Wiseman, Jones and Doherty in 2006 and 2007. In these papers they provided operation definitions of entanglement, steering and Bell nonlocality and used these to demonstrate that for mixed states, Bell nonlocality is strictly stronger than steering which, in turn, is strictly stronger than entanglement.

A more geometric way to understand steering has been proposed in the form of Quantum Steering Ellipsoids [27]. These correspond to a faithful generalisation of the Bloch sphere to a two qubit system, and has led to a geometric definition of separability and provided insights into the structure of mixed state entanglement.

In the last few years there has also been a growing interest in multipartite steering. One of the first papers to consider this was the 2010 paper by Cavalcanti et al.[28] who attempted to build on the ideas originally proposed by Wiseman, Jones and Doherty [25],[26]. However, a very recent paper by Reid and He [29] has pointed out that the procedure used in [28] did not always ensure that nonlocality was shared among all observers. Instead Reid and

He proposed an inductive model which they used to verify n-partite steering for the n-dimensional counterparts of the GHZ state in both discrete and continuous variable Gaussian systems. Finally, another paper published this year by Augusiak et al. [30] showed that entanglement is inequivalent to Bell nonlocality and steering for any multipartite system.

4.1 Experimental evidence for Steering

The experimental demonstration of quantum steering has, perhaps, a surprisingly long history considering that steering was only relatively recently given an operational definition. The first paper to experimentally demonstrate steering appears to have been Z. Ou et al. [31] in 1992 using continuous variable optical beams. Since then there have been many other experiments that have also provided experimental confirmation of steering. Of particular interest is the work of Bowen et al. [32] who in 2003 demonstrated that quantum steering in the Gaussian regime is more demanding than just establishing entanglement.

Recent confirmation of steering in the continuous variable regime includes Samblowski et al. [33] in 2010, and Steinlechner et al. [34] in 2013. The later work is of particular note as Steinlechner reported a sixfold increase of the observed steering effect as quantified by the Reid criteria [35] compared to any similar previous experiment and suggested that these results meant that their work was ready for practical applications.

Work has also been carried out in a discrete setting with photons by several groups including by Wittmann et al.[36] in 2011 and Bennet et al.[37] in 2012, with both papers being of considerable significance.

Wittmann's group has the distinction of coming the closest to a truly loophole-free test of EPR steering. They managed to close the fair-sampling loophole by having high detection efficiency and using a form of the steering inequality that took account of null results. By having a large separation of the detectors and using fast quantum random number generators they were also able to close the locality loophole and a specific form of the freedom-of-choice loophole. While significantly in itself this result would also seem to indicate that a loophole-free test of the Bell inequality may not be that far away.

Bennett's group also managed to closed the detection loophole and in addition provided theoretical and experimental evidence that EPR-steering could be rigorously performed even with arbitrarily high losses.

Finally, two recent important papers were Wagner et al.[38] in 2008 and Händchen et al. [39] in 2012, that helped resolve in the affirmative the question of whether the asymmetry in the definition of steering led to any physical consequences. Wagner's group were able to observe an asymmetry in the steering strengths for two-way steering in spatially entangled laser beams. Händchen's group also used two entangled laser beams that they mixed with two vacuum modes, and found that if the vacuum contribution was in a certain range, one-way steering was possible whereby one party could steer the states of the other but not vice-versa.

4.2 Bell's Theorem via Steering

Bell's theorem was proved in 1964 by the aforementioned John Bell [10] building on earlier work by David Bohm [11] and Einstein, Podolsky and Rosen [3]. However, it has recently been pointed out [23] that there is a relatively straightforward argument establishing the impossibility of a local hidden variable (LHV) description of quantum mechanics that would have been available to Einstein and Schrödinger in 1936 inspired by their contemplation of quantum steering and the incompleteness of quantum mechanics [40].

The following proof is taken almost verbatim from [23]. It involves a system with two observers, A and B, and what A can infer about how the 'real' state of affairs at the remote system B is changed nonlocally or 'steered', by different measurements made by A, assuming that the laws of quantum mechanics can be taken as valid.

In this proof, system B is described by the two-dimensional maximally mixed[8] state $\rho_B = I/2$, in a local hidden variable theory with the actual physical properties of system B being described by the complete set of variables λ. Both possibilities of pure states either being ontic (corresponding to a def-

[8]The consequences of using a non-maximally mixed state are still to be properly investigated...

inite value of λ) or epistemic (corresponding to a distribution over λ), are now shown to lead to a paradox.

If pure states are ontic, $|x\rangle$ corresponds to a definite value of $\lambda_x \in S_x$ (where S_x is the set of all λ underlying ρ_B) and consequently $|x\rangle$ is associated with the delta function $\delta(\lambda_x)$. Assuming that steering results in one of two pairs of orthogonal states $|x\rangle$, $|X\rangle$ or $|y\rangle$, $|Y\rangle$ with $0 < |\langle x|y\rangle|^2 < 1$ so that

$$\rho_B = \frac{1}{2}|x\rangle\langle x| + \frac{1}{2}|X\rangle\langle X| = \frac{1}{2}|y\rangle\langle y| + \frac{1}{2}|Y\rangle\langle Y|$$

the assumption of locality ensures that $S_{\rho_B} = S_x \cup S_X = S_y \cup S_Y$ so one of the outcomes $|x\rangle\langle x|$, $|X\rangle\langle X|$, $|y\rangle\langle y|$, $|Y\rangle\langle Y|$ will always be measured.

Moreover locality enforces preparation noncontextuality [41], so that for an ontic interpretation of pure states to be consistent two different preparation procedures leading to the same mixed state must be described by different distributions over the hidden variables. Here we have

$$\nu_1 = \frac{1}{2}\,\delta(\lambda_x) + \frac{1}{2}\,\delta(\lambda_X)$$

$$\nu_2 = \frac{1}{2}\,\delta(\lambda_y) + \frac{1}{2}\,\delta(\lambda_Y)$$

where ν_1 and ν_2 are both valid hidden variable descriptions of ρ_B. Locality also ensures that the initial distribution $\nu(\lambda)$ cannot be affected by the measurement at A, so we must have $\nu_1 = \nu_2$ which implies:

$$\nu = \frac{1}{2}\,\delta(\lambda_x) + \frac{1}{2}\,\delta(\lambda_X) = \frac{1}{2}\,\delta(\lambda_y) + \frac{1}{2}\,\delta(\lambda_Y)$$

However this is a contradiction given that the ontic interpretation requires $\lambda_x \neq \lambda_X \neq \lambda_y \neq \lambda_Y$.

For the other possibility that pure quantum states are epistemic so that $x(\lambda)$ is a distribution over S_x for the state $|x\rangle$, locality still ensures that

$$\nu(\lambda) = \frac{1}{2}\,x(\lambda) + \frac{1}{2}\,X(\lambda) = \frac{1}{2}\,y(\lambda) + \frac{1}{2}\,Y(\lambda)$$

where the distributions $x(\lambda)$ and $y(\lambda)$ are non-distinct since if $S_y \subset S_X$ then the probability of obtaining $|x\rangle\langle x|$ when the system was in state $|y\rangle$ would be zero contrary to our previous assumption.

In the region $S_1 = S_x \cap S_y$ we must therefore have:

$$\int_{S_x} d\lambda \ y(\lambda) = \int_{S_1} d\lambda \ y(\lambda) = |\langle x|y\rangle|^2 \equiv \alpha \tag{3}$$

and similarly for $S_2 = S_x \cap S_Y$, $S_3 = S_X \cap S_y$ and $S_4 = S_X \cap S_Y$.

Defining

$$x_j \equiv \int_{S_j} d\lambda \ x(\lambda), \qquad j = 1, \ldots, 4$$

and integrating $\nu(\lambda)$ over these regions we find the following constraints:

$$\nu_j \ = \ \frac{1}{2}\, x_j + \frac{1}{2}\, X_j \ \ = \ \ \frac{1}{2}\, y_j + \frac{1}{2}\, Y_j, \qquad j = 1, \ldots, 4 \tag{4}$$

Using (3) and its sibling equations we now obtain

$$x_1 = y_1 = X_4 = Y_4 = \alpha$$

$$x_2 = y_3 = X_3 = Y_2 = 1 - \alpha$$

with all other values zero. Therefore from (4) we find that $\nu_1 = \nu_4 = \alpha/2$ and $\nu_2 = \nu_3 = (1 - \alpha)/2$.

The contradiction is now obtained by considering a third set of orthogonal states $|z\rangle$, $|Z\rangle$ which by the steering theorem can also be steered to via a measurement on A and have equal overlap with the states $|x\rangle$ and $|y\rangle$ so that

$$|\langle z|x\rangle|^2 = |\langle z|y\rangle|^2 = |\langle Z|X\rangle|^2 = |\langle Z|Y\rangle|^2 \equiv \beta = \frac{1}{2}(1 + \sqrt{\alpha})$$

where the final term is the prediction from quantum mechanics. This implies that

$$\begin{aligned} z_1 + z_2 = z_1 + z_3 &= \beta \\ z_2 + z_4 = z_3 + z_4 &= 1 - \beta \\ Z_1 + Z_2 = Z_1 + Z_3 &= 1 - \beta \\ Z_2 + Z_4 = Z_3 + Z_4 &= \beta \end{aligned}$$

which has the solution $z_2 = z_3$ and $Z_2 = Z_3$.

However we must also have

$$\nu_j = \frac{1}{2} z_j + \frac{1}{2} Z_j \qquad j = 1, \ldots, 4$$

but there is no way to solve these equations for non-negative values of z_j and Z_j. An independent set of solutions is given by

$$\begin{aligned} z_1 + z_2 = Z_2 + Z_4 &= \beta \\ z_2 + z_4 = Z_1 + Z_2 &= 1 - \beta \\ z_1 + Z_1 &= \alpha \end{aligned}$$

This implies

$$Z_1 = \alpha - z_1 = \alpha - (\beta - z_2) = \alpha - \beta + (1 - \beta - z_4) = 1 - 2\beta + \alpha - z_4$$

which using $\beta = \frac{1}{2}(1 + \sqrt{\alpha})$ gives

$$Z_1 = \alpha - \sqrt{\alpha} - z_4$$

which is negative for $0 < \alpha$, $z_4 \leq 1$.

This contradiction shows the fundamental dichotomy between local realism and quantum mechanics.

However the most interesting aspect about this proof is not that it provides another way to demonstrate the tension between local realism and quantum mechanics, which after all is now widely known. Instead its significance lies in that it provides a striking example of how steering can be used to solve problems regarding Bell non-locality while using no elements that were not potentially available to Einstein and Schrödinger in 1935 and 1936 when they were first corresponding about this issues.

4.3 Quantum Key Distribution

Bell's theorem and the subsequent experimental evidence that nature possessed quantum correlations stronger than are classically allowed led to an interest in using these correlations for the secure transmission of information and the consequent discovery of quantum key distribution (QKD) protocols. However, although QKD was initially associated purely with Bell nonlocality, recent work has also highlighted the important role that steering plays in this field.

The term, quantum key distribution, is used to describe a variety of protocols that enable the provably secure distribution of private information, provided only that principles of quantum mechanics are valid. Two parties can use QKD over a public channel to generate a random key known only to themselves with the only requirement being that the qubits are communicated with an error rate lower than a certain threshold. Once obtained, such a key can then be used with any algorithm to encrypt a message. In particular, if a QKD-generated key is used as a one-time pad where every bit of the source file is encrypted by combining it using modular addition with the corresponding bit from the QKD-generated key, then such procedure is known to be provably secure [42].

The fundamental idea underlying QKD is that in quantum mechanics a measurement of a quantum system will, in general, disturb the system. More precisely (as shown in section 12.18 of [1]), given two non-orthogonal quantum states, information can only gained at the cost of introducing a disturbance in the signal. Consequently two parties, Alice and Bob, can take advantage of this by transmitting non-orthogonal qubit states between themselves. By measuring the disturbance in test qubits randomly scattered amongst their data qubits they can establish an upper bound for any eavesdropping carried out by any third party (whom we shall not so arbitrarily name Eve). In general, of course, much or even all of the loss in fidelity may be due to noise, but to be provably secure, they must assume that all the loss is a result of eavesdropping.

The two best known QKD protocols are BB84 protocol [43] which was developed in 1984 by Charles Bennet and Gilles Brassard, and the E91 protocol [44] developed by Artur Ekert in 1991. We briefly review the idea behind the E91 protocol as it is more straightforward and also as its original proof of security involved testing for a violation of Bell's inequality to detect eavesdropping. E91 uses entangled pairs of photons, with one photon from each pair being held by Alice and the other by Bob, that are in the joint state:

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

so that photons' polarization for A and B are perfectly correlated. This could be arranged in many ways: Alice and Bob might have previously met and stored the pairs till now, Alice could prepare the states and then send Bob his photon or vice-versa, or the states could have been prepared and sent by a trusted third party. To detect any eavesdropping, Alice and Bob simply

use a random subset of their pairs to check if Bell's inequality is violated. From their measurements in jointly determined random bases, Alice and Bob obtain the correlated classical bit strings from which they can generate a random key known only to themselves.

If the measured level of disturbance is above a certain threshold that depends on the exact procedures and setup used, then Alice and Bob must begin this process anew. If, however, the measured level of disturbance is below the threshold, Alice and Bob now then perform two procedures known as information reconciliation and privacy amplification to increase the correlation between their keys while also decreasing Eve's information about it to any desired level.

Information reconciliation refers to an error-correction protocol conducted over a public channel that attempts to create increasingly correlated shared keys whilst minimizing the amount of information Eve can obtain about these keys. One commonly used procedure is the cascade protocol [45] that operates in an iterative fashion over several stages. Each stage begins with Alice and Bob subdividing both their keys into blocks and then comparing the parity of each of these blocks in turn. Should a difference in parity be detected for a block then the error has to be found and reconciled using a binary search. In the event that an error is found lying in a block from a previous stage that had correct parity, then that block must have another error which must also be found and reconciled. This process is then repeated until every block has been compared, and all the detected errors have been reconciled. For the next stage, Alice and Bob both rearrange their keys in an identical random fashion, and repeat this procedure. By increasing the number of stages Alice and Bob can increase the probability that their keys are identical to arbitrarily close to one. Unfortunately in the process Eve will now have additional information about the shared key from the parity information that was exchanged over the public channel.

Consequently, Alice and Bob must now use a process called privacy amplification to reduce Eve's partial information about the shared key to arbitrarily low levels. Privacy amplification uses the shared key obtained using information reconciliation to to produce another shorter key that Eve will have less information about. One way of doing this is by using a universal hash function that is randomly chosen from a public set of such functions. This takes as input a string equal to the length of the shared key and outputs a string of a shorter chosen length. The value of the length of the shorter key

must be determined by the maximum amount of information Eve could have obtained from her eavesdropping on both the original key generation and the information reconciliation procedures. The final result is that Alice and Bob will now have a shared key that Eve has only vanishingly small knowledge of, which they can use as the basis for secure private communication.

Having explained the basic ideas of quantum key distribution we can now investigate recent advances in this field that have been made possible by the use of quantum steering.

4.4 Device-Independent Quantum Key Distribution

We have shown that quantum key distribution allows two parties to generate secret keys, provided only that the laws of quantum mechanics hold. However in standard quantum key distribution, an implicit assumption in the proofs of security for various protocols (such as BB84 and E91) is that both parties can completely trust their preparation and measurement apparatuses. This assumption has recently been shown to be a potential security flaw [46], and consequently interest has grown in finding ways to guarantee security with fewer assumptions.

It turns out that this is possible and moreover, that there is a minimum set of assumptions which are those used in Device-Independent QKD (DI-QKD). These assumptions allow two parties to guarantee the security of their system based only on their observed violation of Bell inequalities. However, this comes at the cost that the Bell inequality test requires a very high detection efficiency to ensure that the detection loophole is closed. Recent works such as Branciard et al.[47] have therefore considered a scenario where only one party can trust their measurement apparatus, which corresponds to one-sided Device-Independent QKD (1sDI-QKD). A possible example of when this type of scenario might occur in real life is that of a bank that wishes to use QKD based encryption for communication with its customers. In this case the bank's detection equipment can be expected to be extremely accurate whereas it is likely that the mass produced terminals for its customers will be far less accurate.

The tests of security required for QKD, 1sDI-QKD and DI-QKD correspond respectively to separability, a steering inequality [35], and a Bell inequal-

ity. This follows, as expected, the hierarchy found by Wiseman, Jones and Doherty [25]. In practical situations where data loss has to be taken into account Branciard et al.[47] analysed these three scenarios and found that the less strict theoretical assumptions of 1sDI-QKD, namely the requirement for steering rather than Bell nonlocality, significantly lowered the required detection efficiencies for secure transmissions to a level where they were attainable by current technology.

Furthermore a paper this year by Kocsis et al.[48], using the recent discovery by Wiseman, Cavalcanti and Hall [49] that quantum steering can be verified even in the absence of trust in either party by the use of quantum-refereed steering games, showed that it is possible to adapt this idea to produce a DI-QKD protocol using only quantum steering. Taken together with the evidence from Bennet et al.[37] that steering can be rigorously performed even with arbitrarily high losses this represents a major step forward as it allows the security that previously required Bell locality while only needing the detection efficiencies associated with quantum steering.

This is therefore a good point to conclude, with these remarkable developments in the field of quantum key distribution impressively showcasing both the growing theoretical usefulness and potential practical applications of quantum steering.

5 Conclusion

> *You were born together, and together you shall be forevermore . . . but let there be spaces in your togetherness. And let the winds of the heavens dance between.*
>
> Khalil Gibran

Quantum steering has long been the somewhat neglected member of the triplet consisting of itself, entanglement and Bell nonlocality. While their genesis arose from the same papers by Einstein, Podolsky, Rosen and Schrödinger, for a long time interest in first entanglement and later Bell nonlocality vastly overshadowed that in quantum steering.

This was due in no small measure to the fact that for pure bipartite states and perfect detection, entanglement, steering and Bell nonlocality are equivalent. It was not until it was shown by Werner that for mixed states Bell nonlocality was strictly stronger than entanglement that the nature of the exact role played by steering became relevant. The operation definition of steering recently given by Wiseman, Jones and Doherty and their proof that for mixed states Bell nonlocality is strictly stronger than steering, which in turn is strictly stronger than entanglement, has lead to greatly increased interest as to the exact role played by quantum steering.

Since then there has been numerous advances in this field, both theoretical and practical, including work on multipartite steering and one-way steering. In particular it appears that quantum steering is extremely useful in providing simpler proofs and less experimentally demanding physical tests and applications of Bell-nonlocality, particularly in the area of quantum key distribution.

Nonetheless this is still early days for the field of quantum steering and while it has at long last unmistakably differentiated itself from its close siblings, entanglement and Bell non-locality, there is clearly a great deal of both practical and theoretical interest remaining to be uncovered in this field. Consequently it seems only appropriate to close with a quote by Avvaiyar:

What we have learned
Is like a handful of earth
What we have yet to learn
Is like the whole world.

References

[1] M. Nielsen & I. Chuang, *Quantum Computation and Quantum Information*, CUP (2010).

[2] A. Gleason, *Measures on the closed subspaces of a Hilbert space*, Journal of Mathematics and Mechanics 6: 885-893 (1957).

[3] A. Einstein, B. Podolsky & N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?,* Phys. Rev. 47(10):777-780, (1935).

[4] H. Nikolić, *EPR before EPR: a 1930 Einstein-Bohr thought experiment revisited*, arXiv: quant-ph/1203.1139v4 (2012).

[5] E. Schrödinger, Proc. Camb. Phil. Soc., 31, 555 (1935), Proc. Camb. Phil. Soc. 32, 446 (1936).

[6] O. Nairz, M. Arndt, & A. Zeilinger, *Quantum interference experiments with large molecules*, Amer. Jour. Phys. 71 319-325 (2003).

[7] C. Lee et al, *Entangling macroscopic diamonds at room temperature*, Science 334 (6060): 1253-1256 (2 December 2011).

[8] `en.wikipedia.org/wiki/Timeline_of_quantum_computing`

[9] E. Schrödinger (translated by J. Trimmer), *The present situation in quantum mechanics: A translation of Schrödinger's 'Cat paradox paper',* Proc. Amer. Phil. Soc., 124, 323-338 (1935).
Online version at:
`http://www.tuhh.de/rzt/rzt/it/QM/cat.html`

[10] J. Bell, *On the Einstein-Podolsky-Rosen paradox*, Physics, 1(3):195-200, (1964).

[11] D. Bohm, *Quantum Theory*, Prentice-Hall, New Jersey, (1951).

[12] M. Plenio, *Quantum Mechanics*, Imperial College lecture notes (2002).
Online version at:
`www3.imperial.ac.uk/pls/portallive/docs/1/613904.PDF`

[13] J. Clauser, M. Horne, A. Shimony & R. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. 23 (15): 880-884 (1969).

[14] S. Freedman & J. Clauser, *Experimental Test of Local Hidden-Variable Theories*, Phys. Rev. Lett. 28, 938 (3 April 1972).
Online version at:
dieumsnh.qfb.umich.mx/archivoshistoricosmq/ModernaHist/Freedman.pdf

[15] A. Aspect, P. Grangier & G. Roger, *Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities*, Phys. Rev. Lett. 49, 91 (12 July 1982).
Online version at:
www.qudev.ethz.ch/phys4/studentspresentations/epr/aspect.pdf

[16] M. Rowe et al, *Experimental violation of a Bell's inequality with efficient detection*, Nature 409 (6822): 791-794 (2001).
Online version at:
http://www.nature.com/nature/journal/v409/n6822/full/409791a0.html

[17] A. Zeilinger et al., *Bell violation with entangled photons, free of the fair-sampling assumption*, Nature Advance Online Publication (April 14, 2013).
Online version at:
http://www.nature.com/nature/journal/v497/n7448/full/nature12012.html

[18] C. Erven et al., *Experimental three-photon quantum nonlocality under strict locality conditions*, Nature Photonics 8, 292-296 (2014).
Online version at:
www.wetenschapsforum.nl/index.php?app=core&module=attach&section=attach&attach_id=15488

[19] C. Bennett, et al, *Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels*, Phys. Rev. Lett. 70, 1895–1899 (1993).
Online version at:
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.9405

[20] W. Wootters & Z. Wojciech, *A Single Quantum Cannot be Cloned*, Nature 299: 802-803 (1982).

[21] X. Ma et al, *Quantum teleportation over 143 kilometres using active feed-forward*, Nature 489 7415: 269-273 (2012).

[22] S. Takeda et al, *Deterministic quantum teleportation of photonic quantum bits by a hybrid technique*, arXiv:quant-ph/1402.4895 (2014).

[23] T. Rudolph, *How Einstein and/or Schrödinger should have discovered Bell's theorem in 1936*, arXiv:quant-ph/1206.0004 (2012).

[24] R. Werner, *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys.Rev. A 40:4277-4281, (1989). Online version at:
`www2.fisica.unlp.edu.ar/materias/qc/Sp.pdf`

[25] H. Wiseman, S. Jones & A. Doherty, *Steering, entanglement, nonlocality, and the Einstein-Podolsky Rosen paradox*. Phys. Rev. Lett., 98:140402, arXiv:quant-ph/0612147v3 (2007).

[26] S. Jones, H. Wiseman & A. Doherty, *Entanglement, EPR-correlations, Bell-non-locality and Steering*, Phys. Rev. A 76, 052116, arXiv:quant-ph/0709.0390v2 (2007).

[27] S. Jevtic, M. Pusey, D. Jennings, T. Rudolph, *Quantum Steering Ellipsoids*, Phys. Rev. Lett. 113, 020402, arXiv:quant-ph/1303.4724v2 (2014)

[28] E. Cavalcanti, Q. He, M. Reid & H. Wisemanm, *Unified criteria for multipartite quantum nonlocality*, arXiv:quant-ph/1008.5014v3 (2010).

[29] Q. He & M. Reid, *Genuine multipartite Einstein-Podolsky-Rosen steering*, arXiv:quant-ph/1212.2270v3 (2012).

[30] R. Augusiak et al., *Entanglement and nonlocality are inequivalent for any number of particles*, arXiv:quant-ph/1407.3114v2 (2014).

[31] Z. Ou, S. Pereira & H. Kimble, *Realization of the Einstein-Podolsky-Rosen paradox for continuous variables in nondegenerate parametric amplification*, App. Phys. B 55, Issue 3, 265-278 (September 1992).
Online version at:
`authors.library.caltech.edu/6493/1/OUZprl92.pdf`

[32] W. Bowen, R. Schnabel, P. Lam & T. Ralph, *An experimental investigation of criteria for continuous variable entanglement*,
arXiv:quant-ph/1111.0760v3 (2002)

[33] A. Samblowski et al, *Two Color Entanglement*
arXiv:quant-ph/1011.5766v2 (2010).

[34] S. Steinlechner et al., *Strong Einstein-Podolsky-Rosen steering with unconditional entangled states*, arXiv:quant-ph/1112.0461v3 (2011).

[35] E. Cavalcanti, S. Jones, H. Wiseman & M. D. Reid, *Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox*, Phys. Rev. A. 80, 032112 arXiv:quant-ph/0907.1109v2 (2009).

[36] B. Wittmann et al., *Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering*, arXiv:quant-ph/1111.0760v3 (2011).

[37] A. Bennet et al., *Arbitrarily Loss-Tolerant Einstein-Podolsky-Rosen Steering Allowing a Demonstration over 1 km of Optical Fiber with No Detection Loophole*, Phys. Rev. X 2, 031003 (2012).

[38] K. Wagner et al., *Entangling the Spatial Properties of Laser Beams*, Science Vol. 321 no. 5888 pp. 541-543 (23 July 2008).

[39] Vitus Händchen et al, *Observation of one-way Einstein-Podolsky-Rosen steering*, Nature Photonics 6, 598-601, arXiv:quant-ph/arXiv:1206.4446v1 (2012).

[40] A. Einstein (translated by D. Howard), *Letter to Schrödinger (1935)*, Stud. Hist. Phil. Sci. 16, 171 (1985).

[41] R. Spekkens, *Contextuality for preparations, transformations, and unsharp measurement*s, Phys. Rev. A, 71, 052108, arXiv:quant-ph/0406166v3 (2005).

[42] C. Shannon, *Communication Theory of Secrecy Systems*, Bell Syst. Tech. J. 28, 656–715 (1949).
Online version at:
`netlab.cs.ucla.edu/wiki/files/shannon1949.pdf`

[43] C. Bennett & G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Vol 175, page 8 (1984).
Online version at:
`http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf`

[44] A. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. 67, 661-663 (1991).

[45] G. Brassard & L. Salvail, *Secret key reconciliation by public discussion*, Advances in Cryptology: Eurocrypt 93 Proc. 410-423 (1993)

[46] F. Xu, B. Qi & H. Lo, *Experimental demonstration of phase-remapping attack in a practical quantum key distribution system*, arXiv:quant-ph/arXiv:1005.2376v1 (2010).

[47] C. Branciard et al., *One-sided Device-Independent Quantum Key Distribution: Security, feasibility, and the connection with steering*, arXiv:quant-ph/1109.1435v3 (2012).

[48] S. Kocsis et al., *Experimental device-independent verification of quantum steering*, arXiv:quant-ph/1408.0563v2 (2014)

[49] E. Cavalcanti, M. Hall & H. Wiseman, *Entanglement verification and steering when Alice and Bob cannot be trusted*, Phys. Rev. A 87, 032306, arXiv:quant-ph/ arXiv:1210.6051v2 (2013).