Studies of quantum contextuality, Bell non-locality and their role in quantum key distribution protocols

Jaskaran Singh Nirankari

A thesis submitted for the partial fulfillment of
the degree of Doctor of Philosophy

Department of Physical Sciences
Indian Institute of Science Education & Research Mohali
Knowledge city, Sector 81, SAS Nagar, Manauli PO, Mohali 140306, Punjab, India

June 2021

Declaration

The work presented in this thesis has been carried out by me under the guidance of Prof. Arvind at the Indian Institute of Science Education and Research (IISER) Mohali.

This work has not been submitted in part or in full for a degree, diploma or a fellowship to any other University or Institute. Whenever contributions of others are involved, every effort has been made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Jaskaran Singh Nirankari

Place :
Date :

In my capacity as supervisor of the candidate's PhD thesis work, I certify that the above statements by the candidate are true to the best of my knowledge.

Prof. Arvind
Professor
Department of Physical Sciences
IISER Mohali

Place :
Date :

Acknowledgements

No accomplishment has substance nearly as great as the road to achieve it. My journey to the completion of this thesis is replete with personalities and experiences that helped shape this document to its final form, which, now that I think about it, might be incomprehensible to many of them! It is here that I offer words of gratitude to them for making it as such.

This thesis is a testament to the support of my mother Parvinder Kaur Nirankari, my father Ravee Inder Singh Nirankari and sister Anubhav Preet Kaur Nirankari, who still do not grasp the field that I work in and yet stand by me. They are the backbone to all the works that I have accomplished.

However, this journey would not even have begun, if not for the influences and efforts of my thesis supervisor, Prof. Arvind. I am grateful to him for inducting me in his wonderful research group, providing an open and scientific learning environment and for all the academic and non-academic discussions. I would also like to thank my doctoral committee members, Prof. Kavita Dorai and Dr. Mandip Singh for their help during this journey. I would also like to acknowledge Dr. Sandeep K. Goyal for his innovative ideas and all the discussions that we shared. Dr. Manabendra Nath Bera has also been instrumental in shaping this journey by introducing a completely new field to me. I am also indebted to Dr. Paramdeep Singh for the full-of-life discussions that we shared during tea times.

I would like to acknowledge my international collaborators Dr. Debasis Mondal and Dr. Dagomir Kaszlikowski for inviting me to Singapore and collaboration on scientific projects.

On the administration side, my tenure as a PhD scholar at IISER Mohali was made much smoother by the offices of Dean Academics and Dean R&D. I would especially like to acknowledge the efforts of Anuj for all the hardwork in managing our forms for UGC, India. It would be remiss of me if I did not acknowledge the funding I recieved from UGC, India. To that end, I would also like to thank the Directors of IISER Mohali.

I consider myself extremely fortunate to have worked with a majority of the quantum community at IISER Mohali including most of the group leaders mentioned above. My seniors Dr. Harpreet Singh, Dr. Debmalya Das and Dr. Shruti Dogra have been a great inspiration and a source of jokes, pranks and not-so-true stories. I was entrusted by them to carry out these qualities (especially the latter ones) in the group after their exit and hope that I have done them justice. I would like to acknowledge my group members who have been like an extended family of mine: Rajendra Singh Bhati, Kirtpreet Singh Pannu, Jorawar Singh, Gurvir Singh, Jasmeet Singh, Chandan Kumar, Dileep Singh, Gaikwad Akshay Ramdas, Krishna Shinde, Jyotsana Ojha,

Akanksha Gautam, Vaishali Gulati, Sumit Mishra, Aakash Sherawat, Dr. Arun and Dr. Soumyakanti Bose. The mutton parties that we had as a group were truly unforgettable. I would also like to thank my past group members, Kishor Bharti and Atul Singh Arora for their invigorating discussions.

No acknowledgement of mine can be complete without the honorable mention of Dr. Samridhi Gambhir, Dr. Ayushi Singhania, Mayank Saraswat, Vikash Mittal and Jaskaran Singh (the second one!!) for developing my palatte so that I can no longer eat hostel food two days in a row. I would also like to mention our punjabi group at IISER Mohali which comprises of many of the people above and including Dr. Satnam Singh, Dr. Varinder Singh and Dr. Preetinder Singh. It is because of them that I know more about my culture than I ever did. This journey would have been extremely stressful if not for the IISER community. The time spent with my friends Love Grover, Anmol Arya, Dinesh Jhajharia, Ankit Kumar, Bobby, Pranay Jaiswal and Pankaj will be sorely missed.

Most of the works presented in this thesis would certainly not have been possible without help from various websites like Google, tex.stackexchange, math.stackexchange, physics.stackexchange, wikipedia and various scientific journals. To make them accesible in a smooth fashion the computer department and the library at IISER Mohali have a significant part of my thanks. Lastly, I would like to thank Lala ji for providing us victuals that have been instrumental in making us all feel like true scholars, even though at times we weren't!!

Jaskaran Singh Nirankari

Abstract

This thesis deals with foundational concepts of quantum theory including contextuality and Bell non-locality, and their applications in quantum key distribution (QKD) protocols.

We provide a generalization of the standard notion of quantum contextuality and show that it encompasses a broader range of scenarios which can be deemed (non-)contextual. This generalization is then used to depict a violation of a new non-contextual inequality developed by us. The violation so exhibited can be achieved by a single measurement device, which implements a positive operator valued measure (POVM). This number is significantly smaller than in the current contextual scenarios and is optimal as no further reductions are possible. The new non-contextual (NC) inequalities so developed can be easily generalised further for n-cycle scenarios and any number of sequential measurements.

We then develop a QKD protocol which is based on the principle of contextuality monogamy and show that it is unconditionally secure for individual attacks by an eavesdropper. We use the Klyachko-Can-Binicioglu-Shumovsky (KCBS) scenario to share a secure key among two parties via a prepare and measure QKD scheme. Our protocol does not require the use of entanglement, which is a costly resource to produce, while also allowing a security check via a NC inequality like in the case of Bell inequalities. This is achieved by the principle of contextuality monogamy which forbids an eavesdropper to attain information about the secure key without disturbing the correlations among the parties.

We then apply the same strategy to entropic NC inequalities to show that they can also be used to perform secure QKD. We show when an entropic NC scenario can have a monogamous relationship and how it can be derived using a graph theoretic approach. We apply the principle of monogamy along similar lines as before to show that a device independent security proof of the the protocol is possible. This is unlike the previous approach.

We then analyse the role of Bell-CHSH inequality in entanglement based QKD. More specifically, we show that violation of Bell-CHSH is not a sufficient criteria for security, while it is a necessary one. We construct a geometrical representation of

correlations for two qubits from which it is quite easy to infer the usefulness of various states for QKD. We also analyse the role of local filtering in QKD. States which do not violate the Bell-CHSH inequality can be made useful for QKD after local filtering. However, not all states can be made useful including useless Bell diagonal states.

We finally analyse quantum contextuality in pre- and post-selection scenarios which have gained a lot of traction in recent years. Statistics of various outcomes in these scenarios is determined by the Aharanov-Bergmann-Lebowitz (ABL) rule. We show that this rule is non-contextual in non-paradoxical situations, thereby indicating that it does not entirely capture the essence of quantum theory. We further show that by removing post-selection, it is possible to achieve the maximum violation of KCBS inequality as dictated by quantum theory. This indicates that post-selection is a root cause for paradoxical situations.

The thesis is divided into 7 chapters and is organized as follows. Chapter 2 generalizes the traditional assumption of measurement non-contextuality to encompass more exotic scenarios than what was possible earlier. We detail an operational signature of the same from a single measurement device. Chapter 3 deals with a prepare and measure QKD scheme based on the KCBS inequality and the security of the protocol is proven by the use of contextuality monogamy. In Chapter 4 we analyse application of entropic inequalities in QKD protocols. We provide a graph theoretic formalism to derive their monogamous relationships and then use them to show security of these protocols. In Chapter 5 we examine the role of the Bell-CHSH violation in entanglement based QKD protocols and provide a geometrical representation of all two qubit states with regards to their usefulness in QKD. We also show that only in certain cases local filtering operations can be advantageous in transforming useless states to useful in QKD. In Chapter 6 we investigate the role of contextuality in pre- and post-selection scenarios and show that the famous ABL rule is unable to predict contextual correlations, thereby indicating that it cannot simulate the statistics of quantum theory. In Chapter 7 we offer some concluding remarks and possible future directions of our results.

List of Publications

Published works

1. **Jaskaran Singh** and Arvind *Revealing quantum contextuality using a single measurement device by generalizing measurement non-contextuality*. arXiv: 2102.00410

2. **Jaskaran Singh**, Sibasish Ghosh, Arvind and Sandeep K. Goyal. *Role of Bell violation and local filtering in quantum key distribution*. Phys. Lett. A 127158 (2021)

3. Chandan Kumar, **Jaskaran Singh**, Soumyakanti Bose and Arvind. *Coherence assisted non-Gaussian measurement device independent quantum key distribution*. Phys. Rev. A **100** 052329 (2019)

4. Debasis Mondal, Chandan Datta, **Jaskaran Singh** and Dagomir Kaszlikowski. *Authentication protocol based on collective quantum steering*. Phys. Rev. A **99** 012312 (2019)

5. Dileep Singh, **Jaskaran Singh**, Kavita Dorai and Arvind. *Experimental demonstration of fully contextual correlations on an NMR quantum information processor*. Phys. Rev. A **100** 022109 (2019)

6. **Jaskaran Singh**, Kishor Bharti, Arvind. *Quantum key distribution protocol based on contextuality monogamy*. Phys. Rev. A **95** 062333 (2017)

Under preparation

1. **Jaskaran Singh**, Soumyakanti Bose, Arvind. *Stochastic advantage of non-Gaussian resources in measurement device independent quantum key distribution*.

2. **Jaskaran Singh**, Rajendra Singh Bhati and Arvind. *No contextual advantage in the ABL formalism*.

3. **Jaskaran Singh**, Arvind. *From entropic inequalities to secure quantum key distribution*.

Contents

List of Figures

List of Tables

LIST OF TABLES

Chapter 1

Introduction

Quantum theory has been a prime example of being the most experimentally verified theory, while also lacking a clear cut interpretation. Fundamental concepts like the Heisenberg uncertainity principle, Bell non-locality and contextuality are still bewildering to many researchers, whereas the concept of measurement itself is still not well defined. Several attempts have been made to describe these phenomena leading to numerous applications of the same in various information processing tasks. It has been found that these phenomena, although perplexing allow for certain tasks which are either impossible or cannot be implemented with as much efficiency by using classical theory. Furthermore, these applications have also provided much needed hindsight into the corresponding fundamental concepts. It is along these lines that we focus our work.

This thesis deals with novel operational signatures of quantum contextuality and Bell non-locality in newly developed scenarios while also analysing applications of these standard concepts in various quantum key distribution protocols. We provide an innovative approach to generalize the traditional assumption of measurement non-contextuality to include more situations which can be deemed non-contextual. An interesting example of the same is developed in the form of a single measurement device capable of revealing quantum contextuality, which is hitherto an unexplored concept. In subsequent chapters we apply the traditional notion of measurement non-contextuality, entropic non-contextuality and Bell non-locality to analyse security of various quantum key distribution protocols. It is found that contextuality monogamy plays an important role in proving security of the protocols and not all Bell non-local states are useful for key distribution. Finally we analyse pre and post selection scenarios from the persepective of quantum contextuality and find that the famous ABL rule cannot predict the statistics of a contextual scenario.

In this chapter we introduce the various concepts mentioned above by providing a

technical background to the same. We provide a brief introduction to quantum contextuality, Bell non-locality and quantum key distribution in the subsequent sections.

1.1 Quantum contextuality and Bell's inequalities

In this section we review quantum contextuality and Bell's theorems which are the basic concepts used in the thesis. Specifically, we are interested in different formulations and interpretations of quantum contextuality which include the Kochen-Specker (KS) theorem [1, 2, 3], state independent [4, 5] and state dependent proofs [6] of contextuality and finally Spekkens reformulation of the same [7]. We also take a look at entropic versions of quantum contextuality [8, 9] and finally conclude with a review of the Bell-CHSH inequality [10].

1.1.1 Kochen-Specker theorem

Developed in 1967, the Kochen Specker (KS) theorem [1, 3] states that in a Hilbert space of dimension greater than or equal to 3 it is not always possible to associate definite results to outcomes of projective measurements. Specifically, it is not possible to associate the numerical values 0 or 1 to a certain set of commuting projectors $\{\Pi_i\}$ which satisfies $\sum_i \Pi_i = \mathbb{1}$. The outcomes associated with the projectors, $\nu(\Pi_i) = 0$ or 1 must also satisfy the condition $\sum_i \nu(\Pi_i) = 1$.

The above statements are an integral part of the KS theorem and can be derived by assuming functional consistency of results of measurements which is stated as follows. Consider two operators A and B which commute and therefore can be co-measured. Let the system be prepared in some state $|\psi\rangle$, such that

$$\begin{aligned} A|\psi\rangle &= a|\psi\rangle \quad \text{and} \\ B|\psi\rangle &= b|\psi\rangle, \end{aligned} \tag{1.1}$$

where a and b are the eigenvalues of A and B respectively. Since A and B commute it is also possible to measure any function $f(A, B)$ of the two, such that

$$f(A, B)|\psi\rangle = f(a, b)|\psi\rangle. \tag{1.2}$$

In fact, the above property holds even when A and B do not commute but merely share a simultaneous eigenket $|\psi\rangle$. Therefore, functional consistency requires that if a set of projectors follow $\sum_i \Pi_i = \mathbb{1}$, the outcomes themselves must also sum to unity.

The proof of the original KS theorem [1] requires use of 117 different projectors in a three dimensional Hilbert space. The essence of the proof requires the projectors

to appear in more than one contexts, where the context of an observable is defined as the set of observables being co-measured with it. For each of these defined contexts, the projectors satisfy the function $\sum_i \Pi_i = \mathbb{1}$. Consequently, a numerical value of 1 can be associated to any arbitrary projector in the context, while the rest are assigned the value 0 satisfying functional consistency. The next step in the proof follows when it is assumed that numerical values assigned to the projectors do not depend on the context in which they appear. This is the non-contextuality hypothesis. Following this assumption, one arrives at a contradiction of assignment of numerical values to all projectors according to functional consistency.

A simple and elegant example of the KS theorem can be constructed in a Hilbert space of dimension 4 [3]. Let us consider the example of Peres-Mermin square in which operators are arranged in a square array,

$$\begin{array}{ccc} \mathbb{1}\otimes\sigma_z & \sigma_z\otimes\mathbb{1} & \sigma_z\otimes\sigma_z \\ \sigma_x\otimes\mathbb{1} & \mathbb{1}\otimes\sigma_x & \sigma_x\otimes\sigma_x \\ \sigma_x\otimes\sigma_z & \sigma_z\otimes\sigma_x & \sigma_y\otimes\sigma_y \end{array} \tag{1.3}$$

where each of the operators has eigenvalues ± 1. It can be seen that the operators in each row and column commute and each is a product of the other two (except in the third column which is missing a negative sign).

It is a simple exercise to see that it is not possible to assign each operator a definite outcome of ± 1 which also follows functional consistency, which in this case is the product of two operators. A contradiction of definite outcome assignment arises for the last operator of the third column. This can be seen for the following assignment of outcomes

$$\begin{array}{ccc} +1 & +1 & +1 \\ +1 & +1 & +1 \\ +1 & +1 & \pm 1? \end{array} \tag{1.4}$$

In fact it is seen that any possible assignment of the values ± 1 following functional consistency runs into a contradiction for at least one observable. This indicates that the assumption of non-contextuality does not hold for quantum observables in general.

It is interesting to note that certain models constructed using the quantum formalism have also been analysed for being contextual. Specifically, the pre- and post-selection models in which a quantum state is pre-selected before performing a counterfactual or non-counterfactual measurement of an observable A followed by a post-selection of another quantum state is seen to have context dependency in the form of pre- and post-selection [11]. The probability distribution for the observable A is calculated using a rule eponymously named as the ABL rule and is given in detail in chapter 6.

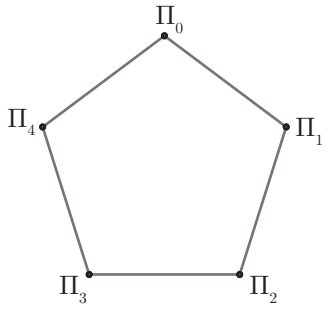

Figure 1.1: The KCBS orthogonality graph as well as the exclusivity graph. Each vertex corresponds to a projector and the edge linking two projectors indicates their orthogonality relationship. The orthogonality relationship for projectors also implies exclusivity.

1.1.2 State dependent proofs of quantum contextuality: KCBS inequality

The KS theorem deals with scenarios in which it is impossible to assign definite outcomes to observables. As such it is based on counterfactual arguments in which the observables are not necessarily measured and the outcomes are assigned counterfactually. It can be argued that the KS theorem is a *logical* proof of contextuality of quantum theory and is not possible to implement in the lab.

For an experimental proof of contextuality of quantum theory, it is required to develop a scenario for which *non-contextual* statistical predictions are not satisfied by quantum theory. Such a scenario was first constructed by Klyachko, Can, Binicioğlu and Shumovsky and is eponymously known as the KCBS scenario [6]. This scenario deals with observables which can be assigned definite outcomes following proper functional consistency and without encountering any contradiction. However, statistical predictions following such a value assignment are not satisfied by considering outcomes from a particular quantum state for the same set of observables. Therefore, quantum theory is deemed to be contextual. Since KCBS inequality is utilized extensively in the present thesis, we detail the scenario in detail below. The KCBS inequality is a test for quantum contextuality in systems with Hilbert space dimension three or more. We review two equivalent formulations of the inequality.

Consider a set of five projectors in a 3-dimensional Hilbert space. The scenario is depicted via an orthogonality graph as given in Figure 1.1. The vertices represent projectors, and two orthogonal projectors are connected by an edge. A pairwise set of projectors, which are mutually orthogonal also commute pairwise. Therefore they can be measured jointly. Such a set of co-measurable observables is called a *context*.

Therefore, as can be seen in the KCBS scenario, every edge between two projectors represents a measurement context and each projector appears in two different contexts. However, a non-contextual model does not differentiate between different contexts of a measurement and deterministically assigns values to the vertices in a context independent fashion.

A deterministic non-contextual model assigns a value 0 or 1 to the i^{th} vertex. The probability that the vertex is assigned a value 1 (0) is denoted by P_i $(1 - P_i)$. Each P_i can take values either 0 or 1. Further, at most one of the vertices connected by an edge can be assigned the value 1 as constrained by the orthogonality relationship which follows from our requirement of functional consistency. For such a non-contextual assignment of outcomes the maximum number of vertices that can be assigned the probability $P_i = 1$ is 2 irrespective of the underlying state. Therefore,

$$\tilde{K} = \frac{1}{5}\sum_{i=0}^{4} P_i \leq \frac{2}{5}. \tag{1.5}$$

This is the KCBS inequality [6], which is a state-dependent test of contextuality and is satisfied by all non-contextual deterministic models. In a quantum mechanical description, given a quantum state $|\psi\rangle$ and the projectors Π_i, the probabilities P_i can be readily calculated. It turns out that the KCBS inequality (1.5) can take values up to $\frac{\sqrt{5}}{5} > \frac{2}{5}$, with the maximum value attained for a particular pure state. Therefore, quantum theory does not allow non-contextual value assignments and is therefore contextual. A particular choice of projectors as in Eq. (3.3) acting on a system in pure state $|\psi\rangle = (0, 0, 1)^T$ does not satisfy the KCBS inequality and attains the maximum quantum bound.

In a more general scenario, where the only functional constraint is the exclusivity principle [12, 13] - that the sum of probabilities for two mutually exclusive events cannot be greater than unity - it is possible to reach the algebraic maximum of the inequality namely,

$$\underset{\{P_i\}}{\text{Max}} \left(\frac{1}{5}\sum_{i=0}^{4} P_i \right) = \frac{1}{2} \tag{1.6}$$

and its attainment goes beyond quantum theory. Unlike inequality (1.5), for a generalized scenario, P_is are allowed to take continuous values in the interval $[0, 1]$.

The correlation can be further analyzed if the observables take values $X_i \in \{-1, +1\}$ and are related to the aforementioned projectors as

$$X_i = 2\Pi_i - I. \tag{1.7}$$

Reformulating Eq. (1.5) in terms of anti-correlations between two observables, we

get [14],

$$K = \frac{1}{5}\sum_{i=0}^{4} P(X_i \neq X_{i+1}) \leq \frac{3}{5}, \tag{1.8}$$

where $i+1$ is taken modulo 5 and $P(X_i \neq X_{i+1})$ denotes the probability that a joint measurement of X_i and X_{i+1} yields anti-correlated outcomes. As before, Eq. (1.8) is obeyed by all deterministic non-contextual models. However, quantum theory can exhibit a violation up to a maximum value,

$$\frac{1}{5}\sum_{i=0}^{4} P_{\mathrm{QM}}(X_i \neq X_{i+1}) = \frac{4\sqrt{5}-5}{5} > \frac{3}{5}. \tag{1.9}$$

It should be noted that the maximum algebraic value of the expression on the left hand side of the KCBS inequality as formulated in Eq. (1.8) is 1.

1.1.3 State independent proofs of quantum contextuality

Formulation of state dependent proofs of quantum contextuality allowed experimental verifications of the same [15, 16, 17]. Such state dependent scenarios are reminiscent of Bell inequalities which show violation for a particular choice of observables and quantum state. However, quantum contextuality allows for something far different.

Following the construction of state dependent proofs of quantum contextuality in which observables can be assigned definite value assignments, it is possible to construct state independent proofs which do not satisfy the statistical predictions of a non-contextual theory for all possible quantum states. The scenario for the same is constructed in a similar fashion as state dependent proofs, in which a set of observables is considered and each observable is a part of more than one context of commuting observables. A definite outcome is assigned to each observable non-contextually according to functional consistency without any contradiction. However, statistical predictions by quantum theory exhibit higher correlations than the non-contextual ones for all possible quantum states [4, 18, 19]. A particularly important proof of the same is by Yu and Oh [5] in a Hilbert space of dimension at least 3 with 13 different projectors.

1.1.4 Graph theoretic approach to quantum contextuality

An extremely useful way of visualizing non-contextual, quantum and generalized correlations was developed by A. Cabello, S. Severini and A. Winters [20]. For this approach they consider only those theories that assign probabilities to *events*. These events could comprise of projectors, measurements, classical value assignments or any other experiment. To any experiment, a graph G can be associated in which events

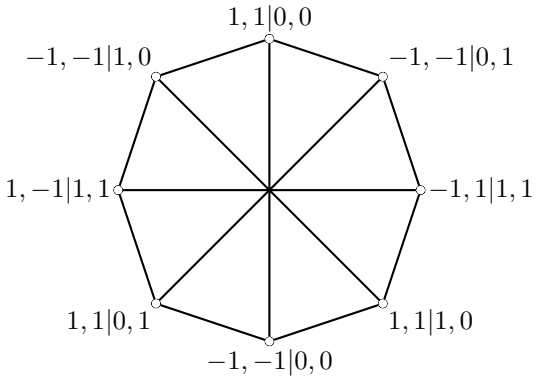

Figure 1.2: Exclusivity graph for the Bell-CHSH inequality. Each vertex represents an event $i,j|x,y$ which in this case corresponds to outcomes i, j of measurements x, y respectively. Two vertices are connected by an edge if they are exclusive to each other.

are represented by vertices and two exclusive vertices are connected by an edge. All vertices connected by an edge are called as adjacent vertices. Such a graph is termed as an exclusivity graph. Any possible experiment can be represented by an exclusivity graph. The graph corresponding to KCBS scenario is similar to the one given in Fig. 1.1, while the graph corresponding to the CHSH inequality is given in 1.2. Using graphs to visualize outcomes of experiments and their correlations makes it easier to analyse whether a particular experiment is capable of revealing contextual or Bell non-local correlations. The result is as follows:

Theorem: Given a correlation experiment with a computable non-contextual or Bell inequality $\mathcal{S}$, the maximum value it takes is given as

$$\mathcal{S} \overset{LHV,NCHV}{\leq} \alpha(G,w) \overset{Q}{\leq} \vartheta(G,w) \overset{E1}{\leq} \alpha^*(G,w), \tag{1.10}$$

where LHV, $NCHV$, Q and $E1$ denote local hidden variable, non-contextual hidden variable, quantum and exclusivity bounds respectively. The graph theoretic constants $\alpha(G,w)$, $\vartheta(G,w)$ and $\alpha^*(G,w)$ are termed as independence number, Lovasz theta number and fractional packing number respectively and can be calculated for a given graph G with weights w assigned to each vertex [12]. The independence number is defined as the maximum number of pairwise vertices which are not connected by an edge, while the fractional packing number is defined as

$$\alpha^*(G,w) = \max \sum_{v\in V} w_v p_v \text{ s.t. } p_v \geq 0 \; \forall v \in V, \; \sum_{v\in C} p_v \leq 1 \; \forall \text{ Cliques } C \subset V, \tag{1.11}$$

where V is the set of all vertices and C is the set of all cliques of the graph. A clique is defined as a set of vertices which are all connected to each other by an edge.

The Lovasz theta number can be calculated as,

$$\vartheta(G, w) = \max \sum_{v \in V} w_v |\langle \psi | \phi_v \rangle|^2, \tag{1.12}$$

where $|\psi\rangle$ is called the handle and $|\phi_i\rangle$ are the projectors assigned to the vertices of the complement of the graph G, denoted by $\bar{G}$. The complementary graph $\bar{G}$ is defined as the graph in which all vertices i, j not adjacent in G are adjacent in $\bar{G}$.

The constants $\alpha(G, w)$ and $\alpha^*(G, w)$ are NP hard to solve, while $\vartheta(G, w)$ can be computed in polynomial time. However, if the complete list of cliques of G are known, then calculating the fractional packing number is as such efficiently computable.

From Eq. (1.10) it is easy to see that any experiment with the property $\alpha(G, w) = \vartheta(G, w)$ is uninteresting as it will not show any quantum advantage over classical correlations. Therefore, it is desirable to identify experiments whose graph theoretic constants follow the relation $\alpha(G, w) < \vartheta(G, w)$.

Well known scenarios including the KCBS and Bell-CHSH inequalities can be formulated by constructing their exclusivity graph and calculating the various constants which yield the correct bounds for LHV, $NCHV$, Q and $E1$.

Using graph theory it is also possible to analyse other interesting properties of various experiments. This includes analysing and designing monogamy relations between different inequalities. This has been achieved in [21, 22] and the general idea is as follows. Consider a commutativity graph in which each vertex is connected to every other vertex with an edge, as in a clique. As shown in [21], cliques in which each vertex corresponds to an observable admit a joint probability distribution over them. Therefore, cliques are incapable of revealing any non-classicality. Another interesting class of graphs is one which there are no cycles of length greater than 3. Such graphs are known as chordal graphs. It can be shown that chordal graphs also admit a joint probability distribution, thereby making them unable to reveal any quantum advantage.

A monogamy relationship between n contextual or Bell like inequalities exists if and only if its vertex clique cover number is $n\alpha$, where the vertex clique cover number is defined as the minimum number of cliques required to cover all the vertices of the graph. The monogamy relationship can be derived by identifying m chordal subgraphs of the joint commutation graph of all the observables such that the sum of their non-contextual or Bell non-local bounds is $n\alpha$. A more detailed analysis is given in Sec. 3.1.1

1.1.5 Bell-CHSH inequality

Much like quantum contextuality, which deals with non-classical features for single indivisible systems, Bell's inequalities deal with non-classical features of systems with

tensor product Hilbert spaces. Moreover, it answers a much more fundamental question of whether the statistics observed in a quantum experiment can be simulated by a classical and local ontological models [23, 24, 25, 26, 27, 28]. Unlike the Bell-KS theorem there is no constraint of having only projective valued measures (PVMs) [29, 30].

According to Einstein et. al. [23], the completeness of quantum mechanical description of reality should be put under scrutiny. They provided a scenario where two spatially separated observers are able to assign outcomes to two non-commuting observables in a counterfactual manner, thereby indicating a paradoxical nature of quantum theory and opening several new avenues of questioning and interpretation of the theory. Their scenario was based on the assumption of an underlying reality that is able to explain the probablistic nature of quantum theory, while a notion of locality was implicitly assumed in the calculations.

In 1964, John Bell's eponymous inequality concluded that one of the aforementioned assumptions has to be wrong and therefore has to be dropped. Traditionally, the assumption of reality is dropped giving rise to the standard interpretations of quantum theory. However, the assumption of locality can also be dropped as is evident in Bohmian mechanics or pilot wave theories [31].

The results of John Bell in the form of a theorem show that nature is inherently probablistic and no local realistic model is able to simulate it. More technicaly, Bell's theorem [24] states that no ontological model which assigns outcomes to measurements in a local manner can reproduce the statistics of quantum theory. A local ontic model assigns measurement outcomes the probability distribution

$$p(x, y|A, B) = \int_{\lambda \in \Lambda} \mu(\lambda) p(x|A, \lambda) p(y|B, \lambda) d\lambda, \tag{1.13}$$

where x, y are the outcomes to observables A and B respectively and λ, $\mu(\lambda)$ are the ontic variables and ontic state respectively as introduced in Sec. 2.2.1. It is assumed that observables are measured on spatially separated systems and therefore cannot influence the outcomes of each other, according to the assumption of locality. The Eq. (1.13) implies that the joint probability distribution $p(x, y|A, B)$ can be factorized into local distributions over the observables A and B given the probability distribution over the ontic variables λ.

The most popular and well studied Bell's inequality is the Bell-CHSH inequality [10] which is defined for the scenario with two parties A and B each having access to two measurement basis. Each of the measurements are assumed to have two outcomes. The scenario is detailed as follows.

The Bell-CHSH inequality quantifies the correlations arising from measurements on two-qubit states. All correlations which violate the inequality are termed as nonlocal as they defy explanation by any local realistic hidden variable model (LRHVM).

1. Introduction

The Bell-CHSH inequality involves two spatially separated parties Alice and Bob sharing an entangled state ρ. Each party performs two measurements, having two outcomes ± 1 on their respective subsystem. Let A_0, A_1 be the measurements performed on Alice's particle and B_0, B_1 be the measurements performed on Bob's particle. We can define a joint operator $\mathcal{B} = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1$ which is called the Bell operator. The Bell-CHSH inequality states that the expectation value S of the Bell operator $\mathcal{B}$ for the classical situations describable by LRHVM is bounded between 2 and -2, i.e.,

$$S \equiv |\mathcal{B}| \leq 2. \tag{1.14}$$

However, some quantum states violate this bound implying that there is no LRHVM for the corresponding physical situations.

An arbitrary two-qubit state ρ can be written in the Hilbert-Schmidt form as [32]

$$\rho = \frac{1}{4}[\mathbb{1} \otimes \mathbb{1} + \boldsymbol{r} \cdot \boldsymbol{\sigma} \otimes \mathbb{1} + \mathbb{1} \otimes \boldsymbol{s} \cdot \boldsymbol{\sigma} + \sum_{i,j=1}^{3} T_{ij} \sigma_i \otimes \sigma_j], \tag{1.15}$$

where $\boldsymbol{r}$ and $\boldsymbol{s}$ are three-dimensional real vectors characterizing the reduced density matrices of the first and the second qubit respectively and T is a 3×3 real matrix representing the correlations between the two qubits. The state ρ can also be parameterized linearly with real parameters as

$$\rho = \frac{1}{4} \sum_{i,j=0}^{3} M_{ij} \sigma_i \otimes \sigma_j, \tag{1.16}$$

where σ_0 is the 2×2 identity matrix and M_{ij} is the Mueller matrix [33], with $M_{00} = \text{Tr}(\rho)$, $M_{0j} = \boldsymbol{s}_j$, $M_{i0} = \boldsymbol{r}_i$ and $M_{ij} = T_{ij}$ $\forall i, j \in \{1, 2, 3\}$. This representation turns out to be quite useful as will become evident.

The measurement operators $\{A_0, A_1\}$ and $\{B_0, B_1\}$ are defined as

$$A_i = \boldsymbol{a}_i \cdot \boldsymbol{\sigma}, \qquad B_i = \boldsymbol{b}_i \cdot \boldsymbol{\sigma}, \tag{1.17}$$

where $\boldsymbol{a}_i$ and $\boldsymbol{b}_i$ are normalized three-dimensional real vectors $\forall i \in \{0, 1\}$. In this new notation, we can calculate the expectation value of the Bell operator as

$$S = \boldsymbol{a}_0^t T \boldsymbol{b}_0 + \boldsymbol{a}_0^t T \boldsymbol{b}_1 + \boldsymbol{a}_1^t T \boldsymbol{b}_0 - \boldsymbol{a}_1^t T \boldsymbol{b}_1. \tag{1.18}$$

Simple algebra shows that for a given two-qubit state ρ the maximum value of S that can be achieved for optimal measurements is [34]

$$\max\{S\} = 2\sqrt{\lambda_1^2 + \lambda_2^2}, \tag{1.19}$$

where λ_1 and λ_2 are the two largest singular values of the correlation matrix T each of which is bounded from above by 1. Therefore, the maximum Bell violation is achieved when $S = 2\sqrt{2}$ [34].

An interesting point to note is that the violation of the Bell-CHSH inequality does not depend on the Bloch vectors $\boldsymbol{r}$ and $\boldsymbol{s}$, but only on the correlation matrix T. Therefore, different states with the same correlation matrix result in the same value of S which itself is determined by the two parameters λ_1 and λ_2 only.

Therefore, if we fix the optimized Bell violation parameter S we obtain a relation between λ_1 and λ_2 giving us a way to describe the family of states with this particular value of Bell violation by only one effective parameter.

1.2 Quantum key distribution

One of the major applications of foundational aspects of quantum theory have been in quantum key distribution (QKD) protocols. Fundamental issues like Bell-nonlocality, contextuality, Heisenberg uncertainty, no cloning theorem, to name a few are found to be extensively useful in quantum key distribution schemes.

A typical cryptographic scheme entails encoding and decoding of secret messages between at least two parties. This encoding and decoding of messages is done via a "key" shared between the parties prior to the relay of messages. However, the distribution of the key is in itself a cryptographic task and is typically known as a key distribution scheme. The communication between parties is deemed secure so long as the key is not known to any adversary. Having knowledge of the key, the adversary can encode or decode the messages being transmitted, thereby compromising the security. Thus, the problem of secure communication can be tackled to a large extent if the parties are able to share a secure key.

Classical key distribution schemes utilize computationally hard to solve mathematical problems like prime factorization. Many of these problems are known to be NP hard, meaning the time required to solve them grows exponentially with the size of the problem. However, a particular solution can be easily verified to be correct or not. The application of these difficult problems for security of key distribution protocols is only valid if an eavesdropper is assumed to have limited computational power.

However, with the advent of quantum computation, some of these hard to solve problems can now be easily addressed on quantum information processors. Therefore, an eavesdropper with access to the same could, in principle, break the prevalent key distribution schemes quite easily.

On the other hand QKD protocols are based on fundamental physical principles which cannot be violated, rather than on difficulty of some computational problem.

This removes the possibility of achieving a possible solution to the problem by using better algorithms, technology or higher computational power. These physical principles place a constraint on the information about the key that can be gained by an eavesdropper and the noise that is introduced in the system as a consequence of it. By measuring the signal to noise ratio, it is thus possible to check for the existence of an eavesdropper.

QKD protocols fall into three major categories:

- Prepare and measure schemes: In these schemes one of the parties encodes the key by preparing one of several pre-defined quantum states. The state is then transmitted to the other party. The recipient party performs one of several pre-defined measurements on the state and the outcomes of these measurements are used to decode the key.

- Entanglement based schemes: These schemes are similar to prepare and measure in that one of the two parties prepares a two qubit entangled state, one of which is retained and the other is transmitted to the other party. It can also be the case that a third party prepares the quantum state and distributes it among the interested parties. Both the interested parties then perform one of the several pre-defined measurements on their respective subsystems. Using the outcomes they share a key.

- Device independent schemes: These schemes are similar to the entanglement based schemes with the difference that no assumptions are made regarding either the preparation or measurement devices with the parties. These protocols are more resilient to several eavesdropping attacks, but offer lower secure keyrates. If no assumption is made only on the measurement devices while the preparation devices are fully characterized, the protocol is termed as measurement device independent. Protocols in which measurement devices are fully characterized while no assumptions are made on the preparation devices are known as semi-device independent. The third category is fully device independent protocols in which no assumption is made on either preparation or measurement devices.

A brief summary of all these protocols which have been studied during this thesis are given in the subsequent sections.

1.2.1 Prepare and measure schemes

The most simple prepare and measure scheme is the famous BB84 protocol, which is also the most widely commercially used QKD scheme. It consists of two interested parties, Alice and Bob, with the former party preparing states in either the $\mathbb{Z}$ basis,

$\{|0\rangle, |1\rangle\}$ or the $\mathbb{X}$ basis, $\{|+\rangle, |-\rangle\}$ with equal probability. Alice assigns a value 0 to the states $|0\rangle$ and $|+\rangle$ and the value 1 to the states $|1\rangle$ and $|-\rangle$. She transmits the states via a quantum channel to Bob. The non-orthogonality of the states ensures that a third untrusted party, Eve, cannot infer the value assigned by Alice to the transmitted state without disturbing it. This is ensured by the Heisenberg uncertainty principle. After receiving the states from Alice, Bob performs a measurement in either $\mathbb{X}$ or $\mathbb{Z}$ basis with equal probability. His choice of basis used is publicly declared.

In a noise free scenario without the presence of an eavesdropper, Bob would perform a measurement in the same basis as Alice's preparation half of the times. Whenever that happens he would observe the same state that Alice transmitted. Therefore, with probability half, Alice and Bob's assignments would be perfectly correlated.

The presence of an eavesdropper Eve can be determined by evaluating the quantum bit error rate (QBER) of the protocol. QBER is defined as the average number of times Alice and Bob performed the protocol correctly, but still observed anti-correlated outcomes instead of correlated. QBER is dependent on the strategy employed by Eve and security of the protocol is determined by the best strategy that can be employed by her.

One of the strategies that can be employed by Eve is to attach an ancillary system to Alice's qubit. Let the ancilla be in the state $|\epsilon\rangle$. In order to gain some information about Alice's system, Eve unitarily evolves the ancilla coupled with Alice's state, thereby entangling them. The total operation is represented as

$$U|\alpha\rangle|\epsilon\rangle = \sqrt{p_\alpha}|\alpha\rangle|\epsilon_{\alpha\alpha}\rangle + \sqrt{Q_\alpha}\left|\alpha^\perp\right\rangle|\epsilon_{\alpha\alpha^\perp}\rangle, \tag{1.20}$$

where $|\alpha\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and $\langle\alpha\left|\alpha^\perp\right\rangle = 0$, p_α denotes the probability for Bob to observe the correct outcome when measuring in the correct basis, while Q_α denotes the probability of getting an erroneous outcome when measuring in the correct basis. The states $|\epsilon_{ij}\rangle$ denote the possible ancillary states of Eve's system. For our purposes, we assume that $Q_\alpha = Q\ \forall\alpha$. This is the case when Eve introduces the same error in the $\mathbb{Z}$ and $\mathbb{X}$ measurements by Bob and is known as a symmetric attack.

The amount of secure key that can be distilled from the protocol is known as the secret key rate and for the BB84 protocol it is given as

$$R = 1 - 2H_2(Q), \tag{1.21}$$

where $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy. It is a routine calculation to see that a non-negative keyrate can be obtained for $Q > 11\%$ and has been shown to be the maximum error rate tolerable by BB84.

1.2.2 Entanglement based schemes

Entanglement based QKD protocols are somewhat similar to prepare and measure schemes. One of the most prominent and easy to understand protocol is the E91 protocol developed by Ekert in 1991. It can be understood as follows.

Two parties Alice and Bob share a maximally entangled two qubit state, for example the Bell singlet state $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. The state could be prepared by one of the parties with one of the subsystems transmitted to the other. Unlike in prepare and measure schemes, Alice and Bob have a choice of randomly performing a measurement in three basis. Alice has the choice: $\mathbb{X}$, $\mathbb{Z}$ and $\frac{1}{\sqrt{2}}(\mathbb{X}+\mathbb{Z})$ basis, while Bob has the choice: $\mathbb{X}$, $\frac{1}{\sqrt{2}}(\mathbb{X}+\mathbb{Z})$ and $\frac{1}{\sqrt{2}}(\mathbb{X}-\mathbb{Z})$ basis. As in BB84, Bob publicly reveals his choice of basis used. For the case when both the parties measured in the same basis, they keep the outcomes as part of the key. In order to check for the presence of an eavesdropper the parties publicly evaluate the Bell-CHSH inequality given by the Bell operator $\mathcal{B}$ in Sec. 1.1.5 with measurement settings $\{\mathbb{X}, \mathbb{Z}\}$ with Alice and $\{\frac{1}{\sqrt{2}}(\mathbb{X}+\mathbb{Z}), \frac{1}{\sqrt{2}}(\mathbb{X}-\mathbb{Z})\}$ with Bob. If the Bell-CHSH inequality is observed to be maximally violated, i.e. $|S| = 2\sqrt{2}$ (1.19), then the parties can be assured that an eavesdropper could not have gleamed any information about the key. In contrast, if the Bell-CHSH inequality is satisfied, an eavesdropper could have been present in the channel.

1.2.3 Measurement device independent schemes

The above mentioned QKD protocols provide excellent key rates with some caveats. In order for the protocols to be secure, it is necessary that the state preparation and measurement devices be fully characterized. For example BB84 protocol is deemed insecure if the states prepared are not single qubits. Furthermore, if the measurement devices are coupled to an ancillary system with the eavesdropper, the security of the protocol may also be compromised. To address some of these various security issues a new and radically different scheme was proposed.

Measurement device independent (MDI) QKD protocols were proposed to bypass the requirement of fully characterizing the measuring devices with Alice and Bob, while the preparation devices still have to be characterized. This limits the possibility of Eve being correlated to the measurement devices to gain information about the secret key.

A general MDI QKD protocol for continuous variable systems proceeds as follows. Two parties Alice and Bob each prepare a two mode squeezed vacuum (TMSV) state with quadrature variances V_A and V_B. For simplicity we assume that $V_A = V_B$.

The pairs of modes are labelled as A_1, A_2 and B_1, B_2 respectively for Alice and

Bob. Alice and Bob both transmit one of their modes, A_2 and B_2, to a third untrusted party Charlie via quantum channels with lengths L_{AC} and L_{BC} respectively, while retaining the modes A_1 and B_1 with themselves. The total transmission length is $L = L_{AC} + L_{BC}$. Charlie interferes the two modes with the help of a beam splitter (BS) which has two output modes C and D. He then performs a homodyne measurement of x quadrature on mode C with outcome X_C and p quadrature on mode D with outcome P_D and publicly announces the obtained outcomes $\{X_C, P_D\}$.

With the publicly available knowledge of $\{X_C, P_D\}$, Bob transforms his retained mode B_1 to B_1' by a displacement operation $D(\alpha)$, where $\alpha = g(X_C + iP_D)$ and g is the gain factor. Consequently, the modes A_1 and B_1' become entangled. Later, Alice and Bob both perform a heterodyne measurement on the modes A_1 and B_1' to obtain the outcomes $\{X_A, P_A\}$ and $\{X_B, P_B\}$ respectively, which end up being correlated. Finally both the parties perform information reconciliation and privacy amplification to obtain the secret key.

1.3 Organization of the thesis

The thesis deals with analysis of operational signatures of quantum contextuality and Bell non-locality and their applications in QKD protocols. It is divided into 7 chapters. A brief introduction to the work presented in them follows as:

Chapter 1

This chapter provides a technical background to the various concepts used in the thesis. This includes introduction to the various formalisms of quantum contextuality, Bell non-locality and quantum key distribution.

Chapter 2

This chapter deals with our result on generalization of the assumption of measurement non-contextuality. We then apply this generalization to show that a single measurement device implementing a positive operator valued measure can exhibit quantum contextuality. This also brings down the number of measurements required.

Chapter 3

In this chapter we provide a quantum key distribution protocol based on the monogamy of KCBS correlations. We quantitatively show that violation of KCBS inequality can

lead to sharing of secure quantum correlations. This is the first known information theoretic application of KCBS inequality and its monogamy relationship.

Chapter 4

In this chapter we develop a quantum key distribution protocol whose security is proven via an evaluation of a entropic non-contextuality inequality. This is done in a similar vein as our earlier result in chapter 3. We show when an entropic monogamous relationship exists and derive it using graph theoretic formalism. We then show that monogamy can be used to prove security of the protocol.

Chapter 5

In this chapter we analyse the role of Bell-CHSH violation in entanglement based quantum key distribution protocols. We find that while it is a necessary condition, it is not a sufficient one for security. We also develop a geometrical representation of all two qubit states with respect to their usefulness for key distribution. Finally, we also analyse the importance of local filtering operations in key distribution scenarios and find that they are useful in certain cases only.

Chapter 6

In this chapter we analyse pre- and post-selection scenarios from the perspective of quantum contextuality. We show that the famous ABL rule to calculate probabilities in these scenarios leads to non-contextual correlations only. However, we find that if post-selection is removed, then the statistics can exhibit contextual behaviour. This indicates that post-selection might be the root of all paradoxes in such scenarios.

Chapter 7

In this chapter we provide a summary of the work done in the thesis and offer some concluding remarks and future directions that can be taken up.

Chapter 2

Revealing quantum contextuality using a single measurement device

2.1 Introduction

Quantum theory is contextual as the outcomes of measurements depend on the context of measurement, namely the set of commuting observables being measured along with the desired measurement [1, 14]. Unlike quantumness of composite systems revealed via Bell type inequalities [10, 25, 35], quantum contextuality can be demonstrated on single indivisible systems and the simplest such scenario involves a three dimensional quantum system and five different projective measurements [6]. While the first proof that quantum theory is contextual was provided by Kochen and Specker [1], involving 117 different projectors in a three dimensional Hilbert space, over time a number of simpler and more systematic ways of revealing quantum contextuality particular the ones based on graph theory have become available [12, 20]. The graph theoretic approach has been successful in identifying new contextual scenarios [4, 5, 13, 36, 37, 38, 39, 40, 41, 42], simplifying formulations of contextuality monogamy [21], contextuality non-locality relationship [22] developing robust self tests [43] and information theoretic applications of contextuality [44, 45, 46].

While most of the analysis in quantum contextuality has been focused on projective measurements, the approach developed by Spekkens [7] generalizes the same to positive-operator-valued measures (POVMs), as well as provides a notion of contextuality for preparations and transformations. With the use of this generalized approach it was possible to bring down the number of measurements required to exhibit contextual behavior to just 3 on a single qubit [47]. Furthermore, this generalization provides a technique for noise-robust experimental verifications of contextuality [47, 48, 49] and

information theoretic applications of quantum situations involving preparation contextuality [50, 51, 52].

While the minimum number of measurements required to reveal quantum contextuality so far is three [47], no physical principle prohibits a smaller number. Could a more generalised approach involving analysis based on sequential applications of POVMs be used to reveal contextuality of quantum situations? Is it possible to generalize Spekkens assumptions to sharpen the contextual non-contextual divide? We take up these questions and show how such generalizations lead to the unearthing of quantum contextuality in more general situations.

In this chapter we propose a notion of measurement non-contextuality (NC) which is a generalization of and is motivated by the assumption of measurement NC developed by Spekkens [7]. As an application of our generalized assumption, we formulate a new experimentally verifiable NC inequality which involves use of a single measurement device that is applied twice sequentially as a signature of quantum contextuality. We show that this inequality is violated by certain quantum scenarios, one of which is explicitly derived. This implies that the underlying ontic models based on our assumption of measurement NC cannot reproduce the statistics of even a single measurement device. Our generalized notion opens up several new and interesting scenarios which are capable of exhibiting correlations that cannot arise from non-contextual or classical ontic models.

2.2 Quantum measurement contextuality

2.2.1 Spekken's approach to quantum contextuality

The traditional notion of quantum contextuality as developed by Kochen and Specker (as detailed in Chapter 1) deals only with assignment of outcomes to projectors in a projective measurement. This approach was considered to be too restricting and is not applicable to various other operations that can be performed in quantum theory. These operations include preparations, transformations and generalized measurements. A much more generalized definition of contextuality was developed by R. Spekkens [7], which we discuss below in brief.

For a generalized definition of contextuality we consider an operational definition of a physical theory, which is defined in terms of preparations, transformations and measurements. The only information that can be inferred from the theory is a probability distribution $p(k|P, T, M)$ of various outcomes k for a given preparation P, transformation T and measurement M.

A notion of equivalence can be defined between the various experimental proce-

dures. Specifically two preparation procedures P and P' are deemed equivalent if

$$p(k|P, M) = p(k|P', M) \quad \forall M. \tag{2.1}$$

Similarly, two measurement procedures M and M' are deemed equivalent if

$$p(k|P, M) = p(k|P, M') \quad \forall P. \tag{2.2}$$

Another similar definition can be made for two transformation procedures T and T' to be deemed equivalent if

$$p(k|P, T, M) = p(k|P, T', M) \quad \forall P, M. \tag{2.3}$$

All procedures that are equivalent are said to belong to that particular equivalence class. Using the above definitions, it is possible to differentiate between various experimental procedures by two features. The first of these features is characterized by defining the equivalence class of the procedure and the second is characterized by properties other than the equivalence class. The second set of features is defined as the *context* of the experimental procedure. It should be noted that by an additional information of the context of the experiment does not correspond to a better prediction of the experimental outcomes.

Using the definition of a *context* it is now possible to define a non-contextual ontological theory. An ontological theory is one which attempts to explain the predictions of the physical theory by assuming that all experimental tests have pre-defined attributes regardless of whether they are being measured or not. These attributes are known as ontic states and can be fully specified by assuming some ontic variables $\lambda \in \Lambda$, which also describe the real state of affairs. In many cases it is not possible to measure the ontic variables and they are aptly named as hidden variables. As a trivial example, quantum states can be assumed to be their own ontic states without any ontic variables λ.

In an ontological model, preparation procedures are defined as preparations of the ontic state of the system. It is possible that the ontic variables might only define a probability distribution over the various ontic states for the physical system to be in. Thus the preparation procedure is then given by a distribution $\mu_P(\lambda)$, such that $\mu_P(\lambda) \geq 0$ $\forall \lambda \in \Lambda$ and $\int_{\lambda \in \Lambda} \mu_P(\lambda) d\lambda = 1 \; \forall P$.

In a similar fashion, a measurement procedure is defined as a measurement of the ontic state of the system in an ontological model. As before, it might only be possible to infer a probability distribution over the ontic states for the physical system to be in. Thus measurement procedures are given by an indicator function $\xi_{k,M}(\lambda)$, which is a function of λ depending upon the outcome k and measurement procedure M, such that $\sum_k \xi_{k,M}(\lambda) = 1 \; \forall \lambda \in \Lambda$.

It is required that the predictions of the ontological model must align with those of the operational model. Therefore, we have

$$p(k|P,M) = \int_{\lambda\in\Lambda} \mu_p(\lambda)\xi_{k,M}(\lambda)d\lambda \quad \forall P,\ M. \tag{2.4}$$

In an ontological model an assumption of non-contextuality based on an operational definition can be made for preparation, transformations and measurements. An ontological model is said to be preparation non-contextual if the representation of every preparation procedure is independent of the context, and instead only depends on the corresponding equivalence class. Specifically,

$$\begin{aligned} &p(k|P,M) = p(k|P',M) \quad \forall M, \\ \implies &\mu_P(\lambda) = \mu_{P'}(\lambda) \quad \forall \lambda \in \Lambda. \end{aligned} \tag{2.5}$$

This implication is known as the assumption of preparation non-contextuality. In a similar fashion, the assumption of measurement non-contextuality states that

$$\begin{aligned} &p(k|P,M) = p(k|P,M') \quad \forall P, \\ \implies &\xi_{k,M}(\lambda) = \xi_{k,M'}(\lambda) \quad \forall \lambda \in \Lambda \end{aligned} \tag{2.6}$$

An ontological model which follows any or both of the assumptions of preparation and measurement non-contextuality is termed as non-contextual with respect to that particular experimental procedure. Such an operational definition of non-contextuality allows for testing non-contextuality in many more scenarios [48, 49]and the subsequent tests are found to be robust against noise [53].

2.2.2 Generalized assumption of measurement non-contextuality

We provide a slightly weaker assumption of measurement non-contextuality which leads to several interesting scenarios not possible under the generalized assumption of non-contextuality as conceived by Spekkens. Firstly, we define two measurement procedures, $\mathcal{M}$ and $\mathcal{M}'$ to be *similar* if

$$p(k|\mathcal{M},P) = s.p(k|\mathcal{M}',P) \quad \forall P, \tag{2.7}$$

where s is a known probability distribution independent of $\mathcal{M}$, $\mathcal{M}'$ or P. In this case, both the measurement procedures can be clearly distinguished. Based on the notion of similar measurement procedures we define our weaker assumption of measurement non-contextuality as,

$$p(k|\mathcal{M},P) = s.p(k|\mathcal{M}',P) \implies \xi_{\mathcal{M},k}(\lambda) = s.\xi_{\mathcal{M}',k}(\lambda), \tag{2.8}$$

which states that the ontic response functions corresponding to *similar* measurement outcomes must be the same up to factor s, which is a known probability distribution. We utilize this assumption in the following sections to exemplify a situation where measurement non-contextuality can be revealed using a single measurement, albeit applied twice sequentially.

As an example consider the following situation. Consider two different projective measurements on a single spin-$1/2$ system given as

$$\begin{aligned} \mathcal{M}_Z &:= \{|0\rangle\langle 0|, |1\rangle\langle 1|\}, \\ \mathcal{M}_X &:= \{|+\rangle\langle +|, |-\rangle\langle -|\}, \end{aligned} \tag{2.9}$$

where $|0\rangle$ and $|1\rangle$ are the eigenkets of Pauli spin-Z, and $|+\rangle$ and $|-\rangle$ are the eigenkets of Pauli spin-X operator.

We define another POVM measurement $\mathcal{M}_{ZX}$ as,

$$\mathcal{M}_{ZX} := \{s|0\rangle\langle 0|, s|1\rangle\langle 1|, (1-s)|+\rangle\langle +|, (1-s)|-\rangle\langle -|\}, \tag{2.10}$$

where $s \in \mathcal{S}$ is sampled from some known classical probability distribution $\mathcal{S}$. The above measurement can be thought of as performing the $\mathcal{M}_Z$ measurement with probability s and $\mathcal{M}_X$ with probability $(1-s)$ on some state ρ while ignoring the information about which measurement was performed at each instant.

Spekkens' notion of the assumption of non-contextuality cannot be applied here because the outcomes $|i\rangle\langle i|$, $\forall i \in \{0, 1, +, -\}$ are clearly distinguishable from the outcomes $s\,|i\rangle\langle i|$ due to the factor of s. Therefore, according to the traditional notion $\mathcal{M}_Z$ and $\mathcal{M}_{ZX}$ are not two different 'contexts' of the outcomes $|0\rangle\langle 0|$ (or any other outcome respectively).

However, our generalized assumption of measurement non-contextuality for the measurements can be applied to the scenario. Let $\xi_{i,k}$ denote the ontic response function assigned to the outcome k for measurement $i \in \{Z, X, ZX\}$, where,

$$\begin{aligned} \xi_{i,k} &\geq 0, \\ \sum_k \xi_{i,k} &= 1. \end{aligned} \tag{2.11}$$

Consider the outcome $|0\rangle\langle 0|$ appearing in the measurements $\mathcal{M}_Z$ and $\mathcal{M}_{ZX}$. We see that for all possible preparations P,

$$p(|0\rangle\langle 0||\mathcal{M}_Z, P) = s.p(|0\rangle\langle 0||\mathcal{M}_{ZX}, P) \quad \forall P, \tag{2.12}$$

which implies according to our assumption of measurement non-contextuality as

$$\xi_{Z,|0\rangle\langle 0|} = s.\xi_{ZX,|0\rangle\langle 0|}. \tag{2.13}$$

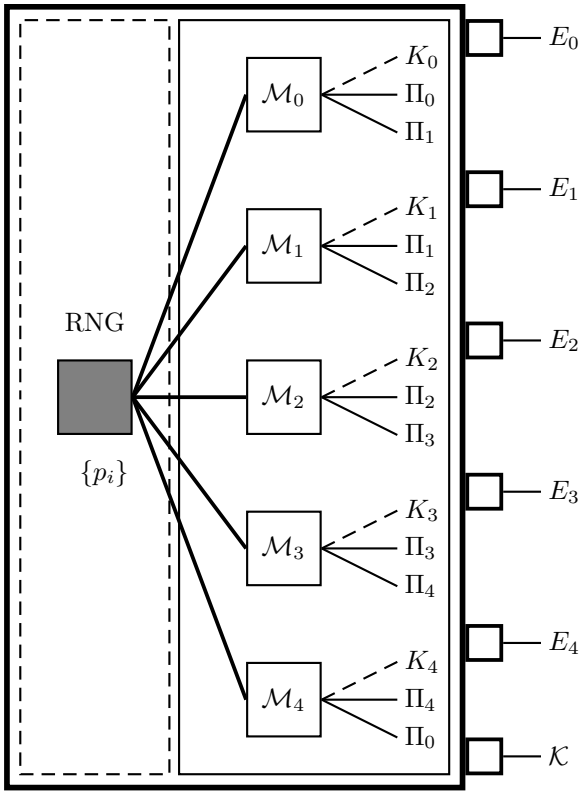

Figure 2.1: A schematic diagram of the two configurations of the measurement device $\mathcal{M}$. In the first configuration, the device samples the measurements $\mathcal{M}_i$ from a random number generator (RNG) with probability p_i and final outcomes E_i and $\mathcal{K}$, while in the second configuration, each measurement $\mathcal{M}_i$ can be performed independently.

A similar analysis holds for all the outcomes for $\mathcal{M}_Z$, $\mathcal{M}_X$ and $\mathcal{M}_{ZX}$

According to our definition even when outcomes are perfectly distinguishable, a notion of 'context' can still be defined. This can be achieved only when the statistics of the outcomes are similar to each other according to Eq. (2.8). This identifies a larger set of contexts for measurements which was not possible earlier. It should be noted that for $s = 1$, our condition transforms into the condition. by Spekkens.

2.2.3 Measurement setup

In this section we describe a measurement procedure able to function in two different configurations. We also formulate an ontologically non-contextual model in order to explain the statistics of both the configurations.

Consider a measurement device which can be made to function in two configura-

tions as shown in Fig 2.1:

C1: The projectors $\{\Pi_i\}$ are sampled from a probability distribution $\{p_i\}$, $i \in \{0, 1, 2, 3, 4\}$, and the device implements the projective measurements $\{\Pi_i, \Pi_{i\oplus1}, K_i\}$, where K_i is taken to complete the measurement and $i \oplus 1$ is taken modulo 5. The projectors $\{\Pi_i\}$ also share the relationship $\text{Tr}(\Pi_i\Pi_{i\oplus1}) = 0$. It is quite easily seen that these projectors are the same as the ones used in the derivation of KCBS inequality. The resultant measurement is then a POVM $\mathcal{M}$ with outcomes,

$$\mathcal{M} : \{E_0, E_1, E_2, E_3, E_4, \mathcal{K}\}, \tag{2.14}$$

where $E_i = (p_i + p_{i\oplus1})\Pi_i$ and $\mathcal{K} = 2\sum_i p_i K_i$ with

$$\sum_{i=0}^{4}(p_i + p_{i\oplus1})\Pi_i \leq \mathbb{1}, \tag{2.15}$$

which is a consequence of completeness of measurement.

C2: By choosing a particular setting i, a projective measurement

$$\mathcal{M}_i : \{\Pi_i, \Pi_{i\oplus1}, K_i\}, \tag{2.16}$$

can also be implemented by the device. This is akin to blocking all measurement outcomes $j \neq i$. From completeness we again have

$$\Pi_i + \Pi_{i\oplus1} \leq \mathbb{1} \quad \forall i. \tag{2.17}$$

There will be 5 such settings corresponding to the projective measurements detailed above.

2.2.4 Ontological description

We now formulate an ontological description of the aforementioned measurement device. For each measurement outcome Π_i from the measurement $\mathcal{M}_i$, there corresponds a response function $\xi_i(\lambda)$, where λs are the ontic variables. Therefore an ontological description of $\mathcal{M}_i$ will have the form

$$\mathcal{M}_{i,\lambda} : \{\xi_i(\lambda), \xi_{i\oplus1}(\lambda), \xi_{K_i}(\lambda)\}. \tag{2.18}$$

From the generalized assumption of measurement non-contextuality, an ontological model of the measurement device in C1 configuration will have the following description,

$$\mathcal{M}_\lambda : \{\xi'_0(\lambda), \xi'_1(\lambda), \xi'_2(\lambda), \xi'_3(\lambda), \xi'_4(\lambda), \xi_{\mathcal{K}}(\lambda)\}, \tag{2.19}$$

where $\xi_i'(\lambda) = (p_i + p_{i\oplus 1})\xi_i(\lambda)$ such that $\{\xi_i(\lambda), \xi_i'(\lambda), \xi_{\mathcal{K}}(\lambda)\} \in [0,1]$ and,

$$\sum_{i=0}^{4}(p_i + p_{i\oplus 1})\xi_i(\lambda) = \sum_{i=0}^{4}\xi_i'(\lambda) \leq 1, \tag{2.20}$$

which is a consequence of Eq. (2.15). Furthermore, by construction, the projectors Π_i and $\Pi_{i\oplus 1}$ are orthogonal, we have,

$$\int_{\lambda\in\Lambda}\xi_i(\lambda)\xi_{i\oplus 1}(\lambda)d\lambda = 0, \tag{2.21}$$

which states that the overlap between the two response functions $\xi_i(\lambda)$ and $\xi_{i\oplus 1}(\lambda)$ is zero.

2.2.5 Quantum signature of measurement contextuality using a single measurement device

In this section we first propose an inequality to be tested by sequential measurements and explicitly derive its maximum non-contextual value. We then show that a quantum description of the same leads to a violation.

Proposition 2.2.1. *The sum of probabilities for obtaining outcomes E_i given the outcome E_j when measurement $\mathcal{M}$ is performed twice sequentially for $p_i = \frac{1}{5}$ is bounded by a non-contextual ontological model as,*

$$\mathcal{C} = \sum_{i,j=0}^{4} p(E_i|E_j) \overset{NC}{\leq} 3.20, \tag{2.22}$$

where $p(E_i|E_j)$ denotes the conditional probability of obtaining outcome E_i given E_j when measurement $\mathcal{M}$ is performed sequentially and NC represents the maximum non-contextual bound.

Proof. In an ontological non-contextual model the probability of obtaining sequential outcomes E_i given E_j represented by response functions $\xi_i(\lambda)$ and $\xi_j(\lambda)$ is given as

$$p(E_i|E_j) = 2\int_{\lambda\in\Lambda} p_i\xi_i(\lambda)\xi_j(\lambda)d\lambda, \tag{2.23}$$

where the ontic state after first measurement is represented by the response function $\xi_j(\lambda)$. Using Eqn. (2.21) and (2.23) we have,

$$\begin{aligned}
\mathcal{C} &= \int_{\lambda\in\Lambda}\left[2\sum_{i=0}^{4}\left(p_i\xi_i^2(\lambda)+2\left(p_i\xi_i(\lambda)\xi_{i\oplus 2}(\lambda)\right)\right)\right]d\lambda \\
&\leq \int_{\lambda\in\Lambda}\left[\frac{2}{5}\sum_{i=0}^{4}\left(\xi_i(\lambda)+2\left(\xi_i(\lambda)\xi_{i\oplus 2}(\lambda)\right)\right)\right]d\lambda \\
&\leq 2+\frac{4}{5}\int_{\lambda\in\Lambda}\left[\begin{pmatrix}\xi_0(\lambda)\left[\xi_2(\lambda)+\xi_3(\lambda)\right]\\ +\xi_1(\lambda)\left[\xi_3(\lambda)+\xi_4(\lambda)\right]\\ +\xi_2(\lambda)\xi_4(\lambda)\end{pmatrix}\right]d\lambda \\
&\leq 2+\frac{4}{5}\int_{\lambda\in\Lambda}\left(\xi_0(\lambda)+\xi_1(\lambda)+\xi_2(\lambda)\xi_4(\lambda)\right)d\lambda \\
&\leq 2+\frac{4}{5}\left(1+\int_{\lambda\in\Lambda}\xi_2(\lambda)\xi_4(\lambda)d\lambda\right) \\
&\leq 3.20,
\end{aligned} \tag{2.24}$$

where for the third inequality we have used $\int_{\lambda\in\Lambda}\xi_i(\lambda)d\lambda = 1$ and for last inequality we have used the fact that overlap between two non-orthogonal states as appearing in the scenario cannot be more than $\frac{1}{2}$. This can be motivated as follows: If the overlap is 1, then $\xi_i(\lambda) = \xi_{i\oplus 2}(\lambda)$, which further implies $\xi_i(\lambda)$ is orthogonal to $\xi_{i\oplus 3}(\lambda)$, which is not allowed. Furthermore, due to symmetry of the problem $\xi_i(\lambda)$ must have an equal overlap with $\xi_{i\oplus 2}(\lambda)$ and $\xi_{i\oplus 3}(\lambda)$. This concludes the proof. □

In order to show that aforementioned non-contextual ontological models is unable to describe quantum statistics, it is enough to provide a single counter-example which violates the inequality (2.22). We explicitly provide the projectors $\Pi_i = |v_i\rangle\langle v_i|$ which will maximally violate the inequality (2.22) and the corresponding violation as follows:

$$
\begin{aligned}
\langle v_0| &= \left(1, 0, \sqrt{\cos\frac{\pi}{5}}\right) \\
\langle v_1| &= \left(\cos\frac{4\pi}{5}, -\sin\frac{4\pi}{5}, \sqrt{\cos\frac{\pi}{5}}\right), \\
\langle v_2| &= \left(\cos\frac{2\pi}{5}, \sin\frac{2\pi}{5}, \sqrt{\cos\frac{\pi}{5}}\right), \\
\langle v_3| &= \left(\cos\frac{2\pi}{5}, -\sin\frac{2\pi}{5}, \sqrt{\cos\frac{\pi}{5}}\right), \\
\langle v_4| &= \left(\cos\frac{4\pi}{5}, \sin\frac{4\pi}{5}, \sqrt{\cos\frac{\pi}{5}}\right).
\end{aligned}
\tag{2.25}
$$

The inequality $\mathcal{C}$ then takes on the value,

$$
\begin{aligned}
\mathcal{C} &= 2\sum_{i=0}^{4}\left(p_i|\langle v_i|v_i\rangle|^2 + 2p_i|\langle v_i|v_{i\oplus 2}\rangle|^2\right) \\
&= 2(1+3-\sqrt{5}) \\
&= 3.52,
\end{aligned}
\tag{2.26}
$$

which is greater than the predicted value for an ontologically non-contextual model. Therefore, such models are unable to predict statistics for even single measurements.

2.3 Conclusions

In this paper we considered a generalizaton of the notion of measurement NC proposed by Spekkens. Such a generalization opens several new interesting scenarios which exhibit a quantum advantage over classical correlations. We have detailed one such scenario in which the statistics of outcomes from a single measurement device is not reproducible from an NC ontic model. Such a scenario has been unearth for the first time to the best of our knowledge. Our results pave the way for future theoretical as well as experimental work to unearth the contextuality of quantum situations. A straightforward extension of our work would entail generalization of the single measurement device scenario to incorporate multiple sequential measurements of the same or different NC scenarios involving n-outcomes and will be taken up elsewhere.

Chapter 3

A quantum key distribution protocol based on contextuality monogamy

3.1 Introduction

Since the advent of quantum theory the existence of pre-defined outcomes for observables has been a matter of heated debate. While Einstein provided a paradox that apparantly showed quantum mechanics to be incomplete [23], it was John Bell who showed that no local ontological model can be compatible with it [24]. This points towards a fundamental departure of the behaviour of quantum correlations from the ones that can be accommodated within classical descriptions. As shown in chapter 1, the contradiction between assignment of predefined measurement-independent values to observables and quantum mechanics was brought forth by Bell's inequalities, which requires composite quantum systems and the assumption of locality, while for single indivisible systems we have the notion of quantum contextuality [1]. The assumption of non-contextuality states that a joint probability distribution over the outcomes of several different measurements on the system exists independently of any possible realisation of the measurements which is also known as the context. However, in the quantum description, there exists contexts corresponding to various different realisations of the measurements and the outcomes in each different context may differ, thereby leading to correlations which cannot be explained by a non-contextual assumption.

A minimal set of 5 observables for a qutrit system was found by Klyachko *et. al.* for which the theoretical value of quantum correlation exceeds the bound (the KCBS inequality) imposed by non-contextual deterministic models [6] as shown in chapter 1. The violation so observed depends on the underlying state on which the measurements

are performed and such models are therefore known as state dependent contextual inequalities.

While at the level of individual measurements quantum mechanics is contextual, the probability distribution for an observable A does not depend upon the context and is not disturbed by other compatible observables being measured. This phenomenon is called the 'no-disturbance' principle and leads to interesting monogamy relations for contextual inequalities [21] which are quite similar to those obeyed by Bell inequalities [54]. These contextual monogamy relations impose constraints on quantum correlations without involving a tensor product structure, which we show to be quite advantageous.

Several non-trivial features of quantum theory play an important role in quantum information processing [55]. In particular, quantum key distribution (QKD) protocols [56] are shown to be fundamentally secure as opposed to their classical counterparts [57, 58, 59, 60, 61, 62, 63, 64, 65, 66] using Bell's inequalities, Heisenberg uncertainity relationship and no cloning theorem.

In this chapter we focus on the prepare and measure class of QKD protocols. One of the prime examples of this scheme is the BB84 [60] protocol which utilizes preparation of 4 different qubit states and measurements in any 2 mutually unbiased bases. However, it has also been shown that prepare and measure QKD protocols can be constructed using any two non-orthogonal qubit states [62]. An extension of the same idea to qutrits [63] to allow four mutually unbiased bases for QKD has also been formulated. On the other hand, the entanglement assisted protocols employ shared entanglement between two parties with the advantage that it is possible to check for security of the protocol based on correlations between the parties via Bell's inequalities which is not possible in the former class of QKD protocols.

While in chapter 2 we explored novel signatures of quantum contextuality, our focus in this chapter is to explore contextual correlations as a resource for QKD. While it has already been exploited for QKD [45], we propose a new protocol based on the KCBS scenario, which is the simplest contextual scenario, and its corresponding monogamy relationships [6, 21]. One of the main advantage of our protocol is that it is a 'prepare and measure scheme' which are experimentally easier to implement, but still allows for a security check based on constraints on correlations shared between the two parties. In fact in our protocol it is the monogamous relationship of the KCBS inequality which is responsible for unconditional security.

We first devise a QKD protocol to share a key between Alice and Bob. We use the KCBS scenario as a resource with post-processing of outcomes allowed on Alice's site. We then derive an appropriate monogamy relation between Alice-Bob and Alice-Eve correlations for the optimal settings of an eavesdropper Eve using the novel graph theoretic approach [20, 21] . From this monogamy relationship, we then explic-

itly derive a bound on the correlations between Alice and Bob to distill a secure key. Our protocol enjoys a distinct advantage of not employing entanglement as a resource which is experimentally difficult to prepare, while still allowing for a security check based on the KCBS inequality. Such a security check is analogous to Bell-type test for security employed in entanglement based protocols. Further, our protocol can be transformed into an entanglement assisted QKD protocol by making suitable adjustments. Although our protocol is not device independent, it adds a new perspective to QKD.

3.1.1 Contextuality monogamy

Given 3 observables A, B and C, such that A can be jointly measured both with B and C (*i.e.* it is compatible with both). In quantum theory the marginal probability distribution of the observable A given by $P(A)$ calculated from the joint probability distributions $P(A, B)$ and $P(A, C)$ is the same:

$$\sum_b P(A = a, B = b) = \sum_c P(A = a, C = c) = P(A = a), \tag{3.1}$$

where a, b and c are the outcomes of the measurements corresponding to the observables A, B and C respectively. This is called the 'no-disturbance' principle and it reduces to the 'no-signaling' principle when an additional assumption is made on the measurements B and C to be performed on spatially separated systems.

The 'no-disturbance' principle can be used to construct contextuality monogamy relationships of a set of observables. This can be achieved if they can be partitioned into disjoint subsets such that each of them is capable of revealing contextuality by themselves but not together. We use graph theoretic approach to derive the monogamous relationships. For KCBS type inequalities, we identify a joint commutation graph representing a set of n KCBS-type inequalities each of which has a non-contextual bound α. This scenario will give rise to a monogamous relationship between the n KCBS inequalities if and only if its vertex clique cover number is $n\alpha$. The vertex clique cover number is defined as the minimum number of cliques required to cover all the vertices of the graph. A clique is a type of graph in which all vertices are connected by an edge.

In order to derive the monogamy relationship we need to identify m chordal subgraphs of the joint commutation graph such that the sum of their non-contextual bounds is $n\alpha$. A chordal graph is a type of graph which does not contain induced cycles of length greater than 3. As is shown in Ref. [21] a chordal graph admits a joint probability distribution and is therefore non-contextual.

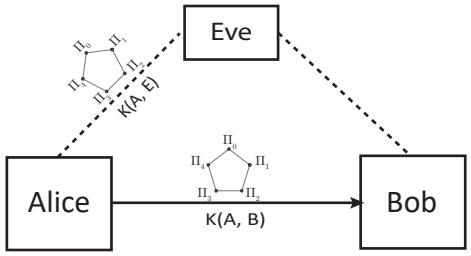

Figure 3.1: Alice and Bob are trying to violate the KCBS inequality [$K(A, B)$], while Eve in her attempts to gain information is trying to violate the same inequality with Alice [$K(A, E)$].

3.2 Quantum key distribution protocol

A typical QKD protocol consists of two interested parties, namely Alice and Bob. We present a QKD protocol based on monogamy of contextuality. Our protocol does not necessarily require entanglement as an initial resource and falls in the purview of prepare and measure schemes. We first derive a monogamous relationship between Alice-Bob and Alice-Eve contextual correlations which we then use to derive a condition for security of the protocol.

3.2.1 Protocol

In a typical key distribution scheme, there are two separated parties Alice and Bob who wish to share a secret key. We assume that both the parties have access to the five projective measurements appearing in the KCBS scenario. From the KCBS graph, Alice randomly selects a vertex i and prepares the corresponding pure state Π_i by performing the respective projective measurement and post-selecting the outcome. She transmits the prepared state to Bob, who also randomly selects a vertex j and performs a measurement $\{\Pi_j, \mathbb{1} - \Pi_j\}$ on it. The measurement settings of Alice and Bob are denoted by i and j respectively. We assign the outcome Π_j a value 1 and the other outcome $I - \Pi_j$ as the value 0. After performing the measurement, Bob publicly announces his setting j. Three distinct cases arise for Bob's outcomes:

C1: $i = j$: By definition Bob is assured to get the outcome value 1 and so records it as such. Alice however notes down the value 0 with herself and publicly announces that the transmission was successful. Thus both the parties share an anticorrelated bit.

C2: i, j are in context but not equal: In this case Bob's setting is in context of Alice's. Since Alice's transmitted state is orthogonal to Bob's chosen projector, he is assured to get the outcome 0 which he notes down as his value. Therefore, Alice notes down the value 1 with herself and publicly announces that the transmission was successful. Thus both the parties again share an anti-correlated bit.

C3: i, j are not in context: In this case Bob's setting does not lie in the context of Alice's. After the public announcement of the setting by Bob, Alice also announces that the transmission was unsuccessful and they try again.

Using the aforementioned protocol, both the parties can securely share a random binary key. Their success probability depends on the chances that Bob's measurements are made in the context or equal to that of Alice's chosen setting. It is seen that they are successful $\frac{3}{5}$ of the times. Whenever Bob uses the correct setting, Alice is able to ensure that they have an anti-correlated key bit. When Bob measures in the same context (but not the same setting as Alice's), Alice notes down the value 1 with herself. In the other case when Bob uses the same setting as Alice's, she notes down the value 0 with herself. This way they always share an anticorrelated bit. At no stage Alice reveals her state. The QKD scenario is depicted in Figure 3.1.

In the ideal scenario without any eavesdropper and noise, Alice and Bob will always get an anti-correlated pair of outcomes whenever they are successful and will therefore violate the KCBS inequality to its algebraic maximum value. It should be noted that they are able to achieve this bound because of post-processing on Alice's side. Whenever, Bob ends up using the measurement settings as Alice, she notes down the value 0 which is not equal to the value assigned to her measurement outcome. Thus, this in no way is a demonstration that quantum theory reaches the algebraic bound of KCBS inequality which in fact it does not.

In the presence of an eavesdropper the violation of the KCBS inequality can be used as a test for security. The presence of Eve decreases the strength of anticorrelations between Alice and Bob. This decrease can be detected by publically sacrificing part of the key for a security check.

In the ideal case the secure key as generated by our protocol is completely anti-correlated but is not completely random. Therefore, the effective length of the key is smaller than the number of successful transmissions. To calculate the actual key rate we compute the Shannon information of the transmitted string. By definition of the protocol, we have $P_0 = \frac{1}{3}$ and $P_1 = \frac{2}{3}$ for the string generated out of successful transmissions. The Shannon information for the same turns out be

$$S = -P_0 \log_2 P_0 - P_1 \log_2 P_1 = 0.9183. \tag{3.2}$$

Below we detail a particular choice of vectors $|v_i\rangle$ (un-normalized) corresponding

QKD protocol	Success probability (per transmission)	Av. key rate in bits (per transmission)
BB84 (2 basis)	$1/2$	0.50
BB84 (3 basis)	$1/3$	0.50
Ekert(EPR pairs)	$1/2$	0.50
3-State [63]	$1/4$	0.50
KCBS	$3/5$	0.55

Table 3.1: The key rate for various QKD protocols in the absence of an eavesdropper. As can be seen the KCBS protocol offers a little higher key rate compared to the other protocols.

to the projectors Π_i, which can be used for the protocol.

$$\begin{aligned}
|v_0\rangle &= \left(1, 0, \sqrt{\cos\frac{\pi}{5}}\right)^T, \\
|v_1\rangle &= \left(\cos\frac{4\pi}{5}, -\sin\frac{4\pi}{5}, \sqrt{\cos\frac{\pi}{5}}\right)^T, \\
|v_2\rangle &= \left(\cos\frac{2\pi}{5}, \sin\frac{2\pi}{5}, \sqrt{\cos\frac{\pi}{5}}\right)^T, \\
|v_3\rangle &= \left(\cos\frac{2\pi}{5}, -\sin\frac{2\pi}{5}, \sqrt{\cos\frac{\pi}{5}}\right)^T, \\
|v_4\rangle &= \left(\cos\frac{4\pi}{5}, \sin\frac{4\pi}{5}, \sqrt{\cos\frac{\pi}{5}}\right)^T,
\end{aligned} \tag{3.3}$$

with,

$$\Pi_i = \frac{|v_i\rangle\langle v_i|}{\langle v_i|v_i\rangle}, \quad i = 0, 1, 2, 3, 4. \tag{3.4}$$

The probability that Bob chooses his measurement setting in the context of Alice's is $\frac{3}{5}$ as stated earlier. Thus, the average key rate generation can be calculated as $\frac{3}{5}S = 0.55$. We tabulate the average key rate of a few QKD protocols in the absence of an eavesdropper in Table 3.1.

It is instructive to note that our proposed prepare and measure QKD protocol can be transformed into an entanglement assisted protocol. In this case let Alice and Bob

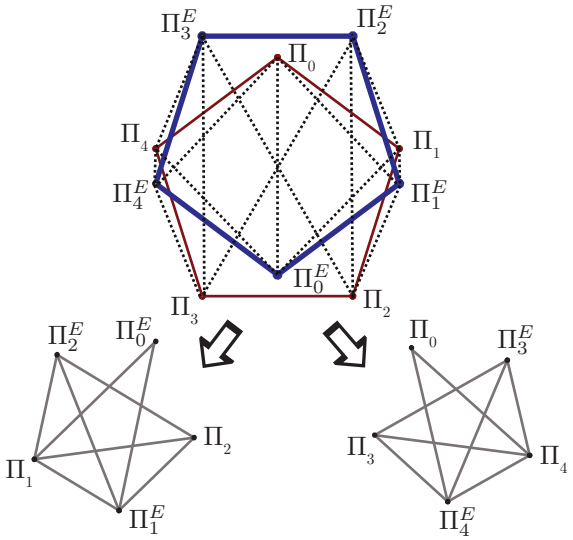

Figure 3.2: Joint commutation graph (top) of Alice-Bob KCBS test (Thin-red) and Alice-Eve KCBS test (Thick-blue) and its decomposition into two chordal subgraphs (below). Dotted edges indicate commutation relation between two projectors belonging to the two different KCBS tests. (color online)

share an isotropic two-qutrit maximally entangled state:

$$|\psi\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^{2} |kk\rangle. \tag{3.5}$$

Alice randomly chooses a measurement setting i and implements the measurement $\{\Pi_i, I - \Pi_i\}$ on her part of the entangled state. For the cases when her states collapses to Π_i, Bob's reduced state is Π_i. This is equivalent to the situation where Alice prepares the state Π_i and transmits it to Bob. Bob also randomly selects a measurement setting j to implement the corresponding measurement. The rest of the protocol proceeds exactly as in the case of prepare and measure scenario as detailed above. We have provided this mapping for the sake of completeness and in our further discussions will continue to consider the prepare and measure scheme.

3.2.2 Derivation of monogamous relationship

Let Alice and Bob be different parties who perform preparations and measurements as detailed in Section 3.2. We consider the possibility of a third untrusted party, Eve, who tries to eavesdrop on the key sharing between them. As will be detailed in Sec-

tion 3.2.3, Eve will have to violate the KCBS inequality with Alice to gain substantial information about the key.

Let us denote the Alice-Bob KCBS test by $\tilde{K}(A,B)$ with projectors $\{\Pi_i\}$ and Alice-Eve KCBS test by $\tilde{K}(A,E)$ with the projectors $\left\{\Pi_i^E\right\}$. For simplicity we have assumed different projectors for the two KCBS tests in order to derive a monogamy relationship, but essentially the measurements by Eve would have to be the same as that of Bob to mimic Alice and Bob's KCBS scenario. In this joint scenario consisting of Alice, Bob and Eve the Π_i^{th} projector is connected by an edge to Π_{i+1}, Π_{i+1}^E, Π_{i-1}, Π_{i-1}^E and Π_i^E, where $i+1$ and $i-1$ are taken modulo 5. The edges in this case denote a commutativity relationship between the two connected vertices. These relationships exist because the projectors used by Eve will follow the same commutation relationships as the original KCBS scenario. By introducing herself in the channel, Eve has created an extended scenario which will have to obey contextuality monogamy due to the no-disturbance principle. The no-disturbance principle guarantees that the marginals calculated from the joint probability distribution are independent of the choice of the joint probability distribution used.

We follow the graph theoretic approach developed to derive generalized monogamy relationships based only on the no-disturbance principle in Ref. [21].

From Fig. 3.2 it can be seen that the joint commutation graph of the QKD protocol satisfies the conditions required for a monogamy relationship to exist between Alice-Bob and Alice-Eve. To derive the relationship we first identify a decomposition of the joint commutation graph into two chordal subgraphs such that each vertex appears at most once in both the subgraphs, as shown in Fig. 3.2. Their maximum non-contextual bound is then be given by the independence number of the subgraph. Therefore,

$$p(\Pi_0^E) + p(\Pi_2) + p(\Pi_1^E) + p(\Pi_1) + p(\Pi_2^E) \leq 2, \tag{3.6}$$

$$p(\Pi_0) + p(\Pi_3) + p(\Pi_3^E) + p(\Pi_4) + p(\Pi_4^E) \leq 2. \tag{3.7}$$

Adding and grouping the terms according to their respective inequalities (Eqn.(1.5)) and normalizing, we get

$$\tilde{K}(A,B) + \tilde{K}(A,E) \leq \frac{4}{5}. \tag{3.8}$$

If the projectors involved in the KCBS tests are transformed according to Eqn. (1.7), then the monogamy relationship reads as

$$K(A,B) + K(A,E) \leq \frac{6}{5}, \tag{3.9}$$

where the monogamous relationship so derived follows directly from the no-disturbance principle and therefore cannot be violated. In other words, the correlations between Alice and Eve are complementary to the correlations between Alice and Bob. If one of

them increases the other correspondingly decreases. One can thus use this to derive conditions for unconditional security as will be shown in the next section.

3.2.3 Secure keyrate analysis

We now prove that our QKD protocol is secure against individual attacks by an eavesdropper limited only by the no-disturbance principle. The best strategy available to Eve would dictate the optimal settings to be used in order to maximize the information gained by Eve about the key. Using the optimal strategy we then prove unconditional security of the protocol which is based on monogamy of the KCBS inequality. The analysis is analogous to the security proof for QKD protocols based on the monogamy of violations of Bell's inequality [59].

Alice and Bob perform the protocol a large number of times. Consequently they share the joint probability distribution $P(a, b|i, j)$, which denotes the probability of Alice and Bob obtaining outcomes $a, b \in \{0, 1\}$ conditioned that their settings are $i, j \in \{0, 1, 2, 3, 4\}$ respectively. In the ideal case they obtain $a \neq b$ when $j = i + 1$, where addition is taken modulo 5. However in the presence of Eve, the secrecy of correlations shared between Alice and Bob has to be ensured even if Eve is distributing the same between them. It is the aim of Eve to obtain as much information about the correlation between Alice and Bob. Eve can accomplish this in several ways including intercepting the information from Alice and re-sending to Bob after performing suitable measurements to gaining knowledge about the key. It is also possible that she is correlated to Alice's preparation device or to Bob's measurement devices. Technically, Eve can have access to a tripartite probability distribution $P(a, b, e|i, j, k)$, where Alice, Bob and Eve obtain outcomes a, b and e when their settings are i, j and k respectively. It is required for of this probability distribution to correspond to the observed correlations between Alice and Bob. In general it is difficult to characterize the optimal strategy of Eve without placing some constraints on her.

For the following security analysis we impose minimal restrictions on Eve. We only assume that she obey the no-disturbance principle and as a consequence her correlations with Alice will be limited by monogamy relations (3.9). Such a constraint is physically well motivated as it is a fundamental law of nature and is obeyed at all times.

We assume that the correlations as observed by Alice and Bob, $P(a, b|i, j)$, is a consequence of marginalizing over the extended tripartite probability distribution

$P(a, b, e|i, j, k)$. This probability distribution is assumed to be distributed by Eve as:

$$\begin{aligned} P(a, b|i, j) &= \sum_e P(a, b, e|i, j, k) \\ &= \sum_e P(e|k) P(a, b|i, j, k, e), \end{aligned} \tag{3.10}$$

where the second equality is a consequence of the no-disturbance principle: Eve's outcome is independent of the measurement settings used by Alice and Bob. We can also analyze the correlations between Alice and Eve in a similar manner:

$$\begin{aligned} P(a, e|i, k) &= \sum_b P(a, b, e|i, j, k) \\ &= \sum_b P(b|j) P(a, e|i, j, k), \end{aligned} \tag{3.11}$$

where the second equality is also a consequence of the no-disturbance principle. This implies that Eve can decide on her outcome based on the settings disclosed by Bob. However, Bob's outcome cannot be used as it is never disclosed in the protocol. A natural question that can be asked now is how strong does the correlations between Alice and Bob need to be such that the protocol is deemed secure.

The QKD scenario involving the eavesdropper now is as follows: Alice and Bob perform the preparations and measurements as detailed in Section 3.2.1, while Eve, constrained only by the no-disturbance principle is assumed to distribute the correlations between them. Whenever Eve distributes the correlation between herself and Alice she uses the same measurement settings as Bob to gain knowledge about the bit of Alice. However, contextuality monogamy limits correlations between Alice and Eve without disturbing the correlations between Alice and Bob significantly as shown in Section 3.2.2.

We assume that Eve is able to perform individual attacks only with no access to quantum or classical memory. Under this paradigm, Eve is only able to attack a single run of the protocol at any time and must perform her operations before the subsequent run. The condition for a secure key distribution between Alice and Bob in terms of Alice-Bob mutual information $I(A : B)$ and Alice-Eve mutual information $I(A : E)$ is given as [67]:

$$I(A : B) > I(A : E). \tag{3.12}$$

For individual attacks and binary outputs of Alice it reduces to the fact that the probability for Bob to guess the bit of Alice, denoted by P_{B}, should be greater than the probability, for Eve to correctly guess the bit of Alice, denoted by P_{E}. The above condition reduces to

$$P_{\mathrm{B}} > P_{\mathrm{E}}. \tag{3.13}$$

From the protocol it is seen that Bob can correctly guess the bit of Alice with probability $P_{\rm B} = K(A, B)$. For $K(A, B) = 1$ Bob has perfect knowledge about the bit of Alice while for $K(A, B) = 0$ he has no knowledge. For any other values of $K(A, B)$ they may have to perform a security check.

We assume that Eve is in possession of a procedure that enables her to distribute correlations according to Eqns. (3.10)-(3.11). The procedure takes as an input k among the five possible settings according to the KCBS scenario and outputs a binary value e. She uses this outcome to determine the bit of Alice when Alice's measurement setting is i. Let the probability that Eve correctly guesses the bit of Alice be denoted by P_{ik}. Since there are 5 possible settings for Alice and Eve each, the average probability for Eve to be successful $P_{\rm E}$ is,

$$\begin{aligned} P_{\rm E} &= \frac{1}{15}\sum_{i=0}^{4}(P_{ii} + P_{ii+1} + P_{ii-1}) \\ &\leq \max\{P_{ii}, P_{ii+1}, P_{ii-1}|\forall\, i\}. \end{aligned} \tag{3.14}$$

The terms in the above equation denote the success probability of Eve when she uses the same setting as Alice and when she measures in the context of Alice, respectively. For all other cases she is unable to gain any useful information. Without loss of generality let us assume that P_{01} is the greatest term appearing in Eqn (3.14). This term corresponds to the success probability of Eve when her setting is 1 and Alice's is 0. However, Alice's setting is unknown to Eve as it is never disclosed in the protocol. Therefore, in this case Eve's best strategy is to always choose her setting to be 1 irrespective of Alice's settings and subsequently try to violate the KCBS inequality with her. The probabilities that appear in the KCBS inequality would then be,

$$\begin{aligned} P(a \neq e|i = 0, k = 1) &= P_{01} = P_{01}, \\ P(a \neq e|i = 1, k = 1) &= P_{11} = 1 - P_{01}, \\ P(a \neq e|i = 2, k = 1) &= P_{21} \leq P_{01}, \\ P(a \neq e|i = 3, k = 1) &= P_{31} \leq P_{01}, \\ P(a \neq e|i = 4, k = 1) &= P_{41} \leq P_{01}. \end{aligned} \tag{3.15}$$

The probability for Eve to get a particular outcome is independent of Alice's choice of settings. Her best strategy to eavesdrop can at most yield all the preceding probabilities to be equal (except the second term which will show a correlation instead of the required anti-correlation) which will maximize $K(A, E)$. Evaluating the KCBS violation for Alice and Eve, we get,

$$K(A, E) = \frac{3}{5}P_{01} + \frac{1}{5} > \frac{3}{5}P_{\rm E} + \frac{1}{5}. \tag{3.16}$$

Using the monogamy relationship given by Eqn. (3.9), we get,

$$\frac{3}{5}P_{\mathrm{E}} + \frac{1}{5} \leq \frac{6}{5} - P_{\mathrm{B}}. \tag{3.17}$$

For the protocol to be secure, Eqn. (3.13) must hold and using the condition (3.17) implies that it happens only if

$$K(A, B) > \frac{5}{8}. \tag{3.18}$$

Therefore the protocol is unconditionally secure if Alice and Bob share KCBS correlation greater than $\frac{5}{8}$. It is worthwhile to mention that the value $\frac{5}{8}$ is lesser than the maximum violation of the KCBS inequality as allowed in quantum theory.

As shown in reference [21] the monogamy relation (3.9) is an optimal condition in the sense that no other stronger conditions exist. This implies that for any QKD protocol (based on violation of KCBS inequality) to be secure, the condition given in Eqn. (3.18) must be satisfied. This quantifies the minimum amount of correlations required for unconditional security. We conjecture that no key distribution scheme based on the violation of the KCBS inequality can perform better than our protocol since we utilize post-processing on Alice's side to extend the violation of the KCBS inequality up to its algebraic maximum.

3.3 Conclusions

In this chapter we presented a QKD protocol which is a direct application of the simplest known test of contextuality namely, the KCBS inequality. The protocol requires for Alice and Bob to achieve the maximum possible anti-correlation amongst themselves in the KCBS scenario. They can achieve the algebraic maximum of the KCBS inequality by allowing Alice to perform post-processing on her recorded bit values after Bob publically declares his measurement setting. We then show that any eavesdropper will have to share a monogamous relationship with Alice and Bob. This severely limits her eavesdropping. For this purpose we derive a monogamy relationship for the optimized settings of Eve which allow her to gain maximum information about the key. We find that the maximum information gained by Eve does not even correspond to the maximum violation of the KCBS inequality as allowed in quantum theory. This unconditional security provides a significant advantage to our protocol since it does not utilize the costly resource of entanglement. Furthermore, unlike other prepare and measure QKD schemes it also allows for a check of security by the violation of the KCBS inequality. This makes our protocol similar to the ones which are based on the violation of Bell's inequalities. Finally, we note that the security of our protocol is a consequence of contextuality monogamy, which is expected to play an interesting role in quantum information processing.

Chapter 4

From entropic inequalities to secure quantum key distribution

4.1 Introduction

It is well known that measurements on quantum states exhibit correlations which defy explanation by a classical theory. The outcomes of measurements performed on spatially separated or even on single indivisible systems may exhibit correlations greater than their apparent classically allowed values. These correlations are termed as Bell non-local [10, 25, 35, 68] or contextual [1, 12, 13, 20, 36], respectively and are studied by means of certain inequalities, a violation [15, 69, 70, 71, 72] of which implies non-classical behavior. The most widely studied inequalities in this context are the Bell-CHSH [10] and KCBS inequality [6], quantifying Bell non-local and contextual correlations, respectively. Quantum correlations have found immense application in quantum information processing tasks including self-testing [73, 74], QKD [75], DIQKD [58, 76] and randomness certification [77]. One of the major advantages of using quantum correlations over their classical counterparts is apparent in QKD where it is shown that the exchanged key can be deemed secure if the correlations violate a Bell's or a non-contextuality inequality [44, 58, 59]. Furthermore, correlations violating a variant of the Bell's inequality, namely Bell-CHSH, are known to provide security independently of the operations of the devices being used to exchange the key. Such type of key distribution schemes are termed as DIQKD [59, 78] and have no analogue in classical theory. Such DIQKD protocols are even secure against an eavesdropper who might have access to correlations stronger than quantum theory, but still limited by the no-signalling principle. These protocols are the pinnacle in secure key distribution schemes made possible by quantum correlations.

Offering a different perspective on quantum correlations, Braunstein and Caves introduced an information theoretic approach to understand non-local correlations [8, 79]. In this formalism, the joint Shannon entropies carried by measurements must satisfy an inequality in order to have a local description of correlations. Subsequently, the work was extended to include non-contextual scenarios [9, 80] as well, and the inequalities are termed as entropic non-contextuality (ENC) inequalities. Since their inception, these inequalities have been studied extensively and have also been realised experimentally [81]. Entropic inequalities offer the added advantage of being independent of the number of outcomes in a measurement. This property makes them suitable candidates for applications in non-locality distillation [80], bilocality scenarios and QKD, the latter of which we explore in this chapter.

The main aim of this chapter is to analyse whether the set of non-local correlations identified for DI security in [58, 59] is unique with respect to different notions of non-locality. To that end we devise a QKD protocol centered around information theoretic Bell's inequalities or ENC inequalities with even number of observables, which we term as entropic key distribution (EKD). Since these inequalities are more strict and fundamentally distinct from standard Bell inequalities, it is expected that a distinct set of correlations should be observed for DI security. However, our results state otherwise.

We analyse the connection between violation of the entropic inequality and correlations between two parties Alice and Bob for increasing number of observables. Using graph theoretic formalism we show that if the correlations between Alice and Bob violate an ENC inequality, then an eavesdropper, Eve, cannot be correlated to Alice (Bob). This leads to the emergence of monogamy relations between the three parties, which we again achieve from a graph theoretic perspective. Using the monogamy relations so derived and the assumption of individual attacks we show that the EKD protocol is secure even against a supraquantum Eve limited only by the no-signalling principle. In effect we derive a simple information theoretic condition to check for DI security, which surprisingly also reproduces the set of correlations as derived in [58, 59] for DI security in the case of Bell-CHSH. Our results show that ENC inequalities can also be applied to QKD in a DI manner.

4.2 n-cycle entropic non-contextuality inequalities

In this section we provide a concise review of entropic inequalities as conceived by Braunstein and Caves [8]. We then provide a brief analysis of the same by way of PR boxes.

Consider an n-cycle commutation graph for which the n vertices and edges repre-

sent observables X_i and their commutation relationship respectively. We assume that a non-contextual joint probability distribution exists over the entire set of observables considered, even though most of them do not commute. It is our aim to construct a condition based on the preceding assumption for which a violation would indicate that such a non-contextual joint probability distribution model does not exist.

The existence of a non-contextual joint probability distribution over the observables X_i implies that it is possible to define a joint Shannon entropy $H(X_0, ..., X_{n-1})$ of them. We can then write

$$H(X_0, X_{n-1}) \leq H(X_0, ..., X_{n-1}), \tag{4.1}$$

where the relationship $H(X) \leq H(X, Y)$ is physically motivated by the fact that two random variables cannot contain less information than a single one of them. Furthermore, with repeated application of the chain rule $H(X, Y) = H(X|Y) + H(Y)$, where $H(X|Y)$ denotes the conditional entropy of observable X given information about observable Y, the right hand side of the inequality can be re-written as,

$$\begin{aligned} H(X_0, ..., X_{n-1}) \leq & H(X_0|X_1, ..., X_{n-1}) + H(X_1|X_2, ...X_{n-1}) + ... \\ & + H(X_{n-2}|X_{n-1}) + H(X_{n-1}) \\ \leq & H(X_0|X_1) + H(X_1|X_2) + ... + H(X_{n-2}|X_{n-1}) + H(X_{n-1}). \end{aligned} \tag{4.2}$$

The second inequality in Eq. (4.2) is a consequence of the relationship $H(X|Y) \leq H(X)$, which implies that conditioning cannot increase the information content of a random variable. Plugging Eq. (4.2) in Eq. (4.1) and using

$$H(X_0|X_{n-1}) = H(X_0, X_{n-1}) - H(X_{n-1}), \tag{4.3}$$

we finally get the required entropic non-contextuality inequality,

$$H_{K_1} : H(X_0|X_{n-1}) \leq H(X_0|X_1) + ...H(X_{n-2}|X_{n-1}). \tag{4.4}$$

A violation of Eq. (4.4) would then indicate that a non-contextual joint probability distribution over the corresponding set of observables does not exist.

It should be noted that no assumptions have been made regarding the nature of the observables X_i. For all intents and purposes they can correspond to projective measurements or POVMs with any number of outcomes. Furthermore, the observables could correspond to local scenarios or non-local, in which case the entropic inequality would be termed as non-contextual or Bell non-local. Since we consider generalized scenarios, we term all entropic inequalities as non-contextual as it subsumes the non-local scenarios as well.

The violation of entropic inequalities (4.4) can also be studied by non-signalling Popescu-Rohrlich (PR) boxes [82]. A PR box is a non-signalling probability distribution that can violate a Bell's inequality up to its algebraic bound. For the CHSH inequality, given by,

$$\langle S\rangle = \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle, \tag{4.5}$$

with maximum classical and quantum bounds equal to 2 and $2\sqrt{2}$ respectively, the PR box that achieves the maximum algebraic value of 4 is given by,

$$P_{PR}(a,b|A_x,B_y) = \frac{1}{4}\left(1+(-1)^{a\oplus b\oplus xy}\right), \tag{4.6}$$

where $P_{PR}(a,b|x,y)$ denotes the probability to obtain outcomes a and b when measurements A_x and B_y are performed and $\oplus$ denotes addition modulo 2. For $n=4$ and $X_i = A_i$ for $i =$ odd and $X_i = B_i$ for $i =$ even, it can be seen that the resultant entropic inequality (4.4), which is analogous to CHSH, does not show a violation for the CHSH PR box. Furthermore, as seen from an entropic point of view, the CHSH PR box is found to be equivalent to the classical probability distribution P_C which saturates the classical bound of the CHSH inequality (4.5), given as,

$$P_C(a,b|A_x,B_y) = \frac{1}{4}\left(1+(-1)^{a\oplus b}\right). \tag{4.7}$$

This interesting behavior of entropic inequalities is due to the fact that they cannot distinguish between perfect correlations and anticorrelations of A_1 and B_1 as they appear in $P_C(a,b|A_1,B_1)$ and $P_{PR}(a,b|A_1,B_1)$ respectively. Entropically, both the probability distributions are equivalent. The maximum possible violation of the entropic inequality (4.4) is then achieved by the non-signalling entropic box P_{EB} [79], given by

$$P_{EB}(a,b|A_x,B_y) = \frac{1}{2}(P_{PR}+P_C), \tag{4.8}$$

which is an equal mixture of the PR box and classical correlations. This probability distribution can be understood as having perfect correlations between the pairs (A_0,B_0), (A_0,B_1), (A_1,B_0) while the last pair (A_1,B_1) is as uncorrelated as possible. It is therefore the case that some scenarios which exhibit a violation of the Bell-CHSH inequality do not show a violation of corresponding entropic CHSH inequality.

The maximum quantum violation can also be analyzed in terms of entropic boxes. We consider a mixture of entropic box defined in Eq. (4.8) with weight v and white noise as,

$$P(a,b|A_x,B_y) = \frac{v}{8}\left(2+(-1)^{a\oplus b}+(-1)^{a\oplus b\oplus xy}\right)+\frac{1-v}{4}. \tag{4.9}$$

The entropic inequality 4.4 for $n = 4$ then takes on the value

$$\begin{aligned} H_{K_1} = 4 + 3\left(\frac{1+v}{2}\right)\log_2\left(\frac{1+v}{4}\right) \\ + 3\left(\frac{1-v}{2}\right)\log_2\left(\frac{1-v}{4}\right) \end{aligned} \tag{4.10}$$

It is seen that for $v > 0.877$ a violation of the above inequality is observed. This indicates that a very small set of two qubit correlations exist for which entropic CHSH inequality is violated, in contrast to the comparatively bigger set of two qubit correlations for Bell-CHSH inequality. In the following sections we show that these correlations are capable of providing a secure key rate.

4.3 Entropic key distribution protocol

In this section we develop the entropic QKD protocol which is based on ENC inequalities (4.4). We first consider a specific case of $n = 4$ observables, which is analogous to the CHSH inequality and then generalize the developed protocol for arbitrary n.

Consider two parties, Alice and Bob, each having two observables each, labelled $\{A_0, A_1\}$ and $\{B_0, B_1\}$, respectively. The choice is such that observables of any one party do not commute. It is also assumed that a measurement of any observable can have arbitrary, but known number of outcomes. In order to share a secure key, it is required that the obtained correlations violate the entropic version of the CHSH inequality which is obtained by taking $n = 4$ in Eq. (4.4) and $X_i = A_i$ for $i =$ odd and $X_i = B_i$ for $i =$ even,

$$H_{K_1} : H(A_1|B_1) - H(A_1|B_0) - H(B_0|A_0) - H(A_0|B_1) \leq 0. \tag{4.11}$$

A violation of the above inequality implies non-existence of a joint probability distribution over all the observables A_x and B_y.

We assume that Alice and Bob share the maximally entangled pure singlet state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \tag{4.12}$$

In order to maximize the violation of the inequality (4.11), the observables of Alice and Bob are assumed to lie in the X-Z plane and correspond to Pauli spin measurements along the unit vectors **a**, **a**′, **b** and **b**′ respectively. The vectors **a**, **b**′, **a**′, **b** are successively separated by an angle $\theta/3$. The corresponding value of the inequality (4.11) is

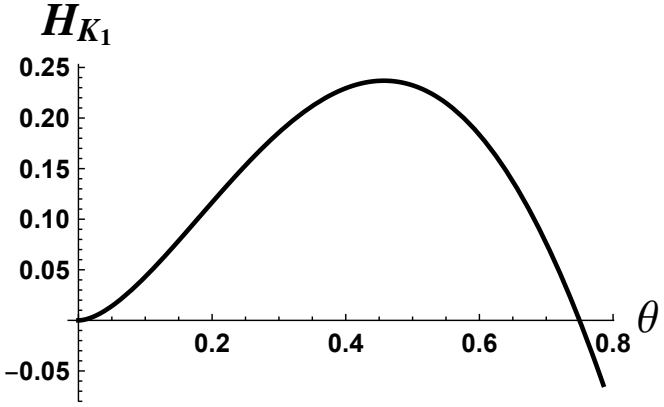

Figure 4.1: The behavior of entropic inequality H_{K_1} (4.13) with respect to the angle θ (taken in radians).

then computed as

$$\begin{aligned} H_{K_1} = 2 &+ 3\sin^2\left(\frac{\theta}{3}\right)\log_2\left(\frac{\sin^2\left(\frac{\theta}{3}\right)}{2}\right) \\ &- \sin^2\theta\log_2\left(\frac{\sin^2\theta}{2}\right) + 3\cos^2\left(\frac{\theta}{3}\right)\log_2\left(\frac{\cos^2\left(\frac{\theta}{3}\right)}{2}\right) \\ &- \cos^2\theta\log_2\left(\frac{\cos^2\theta}{2}\right). \end{aligned} \tag{4.13}$$

The maximum violation, $H_{K_1} = 0.237$ bits is found to occur at $\theta = 0.457$ rads and the corresponding behavior is plotted in Fig. 4.1.

To perform key distribution both the parties choose their state and measurements corresponding to maximum violation as above and then keep their outcomes as part of the raw key. After performing measurements one of the parties, say Bob, publicly announces his choice of basis. It should be noted that even in the ideal noise free case, the parties do not share perfectly correlated outcomes.

The total correlations between Alice and Bob can be analysed by re-writing the inequality (4.11) in terms of mutual information as

$$\begin{aligned} H_{K_1} :& I(A_0 : B_0) + I(A_0 : B_1) \\ &+ I(A_1 : B_0) - I(A_1 : B_1) - H(A_0) - H(B_0) \leq 0, \end{aligned} \tag{4.14}$$

where $I(A_x : B_y)$ denotes the mutual information between the observables A_x and B_y. The total correlations between Alice and Bob is then given by $I(A : B) = I(A_0 : B_0) + I(A_0 : B_1) + I(A_1 : B_0) + I(A_1 : B_1)$. We can now define Alice and Bob's

total correlations in terms of the entropic inequality, H_E as

$$I(A:B) = H_{K_1} + H(A_0) + H(B_0) + 2I(A_1:B_1). \tag{4.15}$$

For the case when Alice and Bob share perfect correlations, e.g. in E91 protocol, then $I(A:B) = 4$ bits. However, in our case due to imperfect correlations, the key rate between Alice and Bob in the absence of any external noise or eavesdropper is $I(A:B) = 2.83$ bits. The loss in total correlations can be explained by noting that a violation of inequality (4.14) requires minimizing the correlations between A_1 and B_1 while maximizing between the rest of the combinations.

The aforementioned protocol can be easily generalized to any even number of observables. It is however, easier to visualise the generalized version in the form of commutativity graphs. In a commutativity graph, each vertex represents an observable, and vertices connected by an edge commute. For the case of even n observables, the graph takes the form of an n-cycle graph with additional edges which connect all of Alice's observables to Bob's observables (due to spatial separation) and each alternate vertex corresponds to an observable with Alice or Bob. As an example consider the graph in Fig. 4.3 for $n = 4$ which represents the entropic CHSH inequality with the addition of an eavesdropper Eve. The protocol remains the same as above, where Alice and Bob select the observables which maximize the violation of the corresponding entropic inequality and randomly perform their respective measurements and store outcomes as part of raw key. In order to perform a security check, they observe the value of the corresponding ENC inequality. The violation and the raw key rate for various values of n are plotted in Fig. 4.2. It is seen that the key rate increases with the number of observables, while also offering a larger region for observing violation of ENC inequality.

4.4 Monogamy of entropic inequalities

In this section we firstly show that the correlations between Alice and Bob violating Eq. (4.11) cannot arise as marginals of a tripartite probability distribution, as conceived by an eavesdropper Eve where she is directly correlated to Alice (Bob). We then go on to show that Alice-Bob and Alice-Eve correlations must follow a monogamous relationship which arises as a consequence of no-signalling principle. We devise necessary conditions for a monogamy relation to exist and elucidate the mechanism to derive the same for a given scenario from a graph theoretic perspective.

A violation of the inequality (4.11) implies that a joint probability distribution cannot exist over the given observables. It can also be shown that a violation of entropic CHSH inequality excludes any tripartite (or n-partite) probability distribution

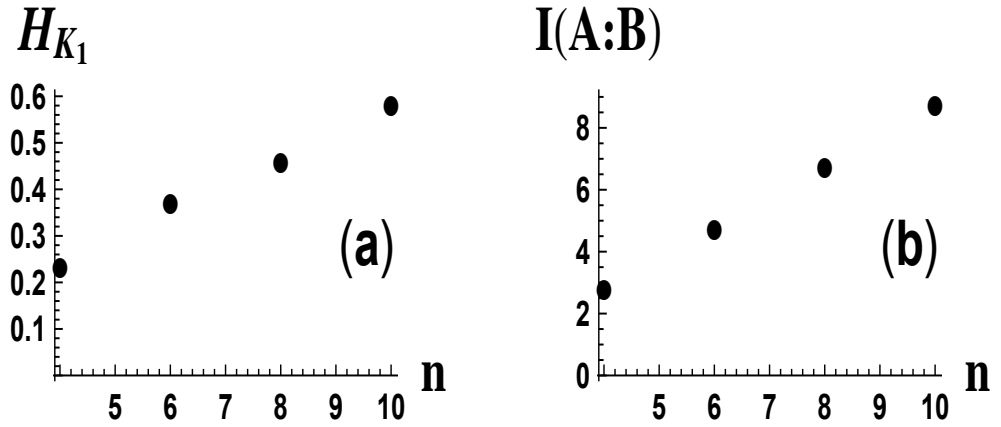

Figure 4.2: (a) Violation of n cycle entropic inequalities for increasing number (even) of observables and (b) raw key rate for increasing number (even) of observables.

$P(a, b, e|A_x, B_y, E)$, in which Eve is directly correlated to Alice, with marginals

$$\begin{aligned} P(a, b|A_x, B_y) &= \sum_e P(a, b, e|A_x, B_y, E) \\ &= \sum_e P(e|E)P(a, b|A_x, B_y, E, e), \end{aligned} \tag{4.16}$$

where $P(a, b|A_x, B_y)$ denotes the joint probability distribution of obtaining outcome a and b when observables A_x and B_y are measured. The second equality arises from the fact that Alice and Bob's inputs cannot influence the outcomes of Eve. We can now prove the following proposition:

Proposition 4.4.1. *A violation of inequality (4.11) implies that a tripartite joint probability distribution, as conceived by Eve to distribute correlations between Alice and Bob and still be correlated with them, cannot exist and for which the observed joint statistics of Alice and Bob arise as marginals.*

Proof. We use graph theoretic framework and a result proven in [21] to elucidate the proof. We consider the commutation graph of the entropic CHSH scenario represented by solid lines in Fig. 4.3. In this graph vertices represent the observables A_i and B_j, and two vertices connected by an edge commute. In order to distribute the correlations between Alice and Bob and satisfying Eq. (4.16), Eve's device or observable(s) must commute with both Alice and Bob's measurements. The resultant graph is found to be chordal. As shown in [21] all chordal graphs admit a joint probability distribution.

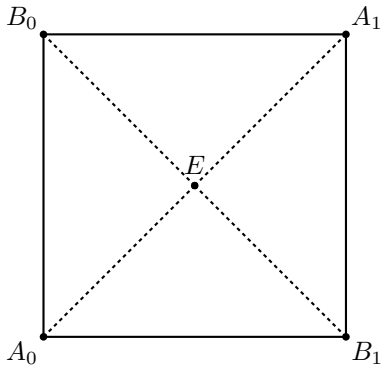

Figure 4.3: A joint commutation graph of Alice-Bob-Eve scenario where Eve uses a procedure E to distribute the required correlations between Alice and Bob. Solid lines represent the CHSH commutation graph between Alice and Bob in which observables are represented with vertices and commuting vertices are connected by an edge. The dashed lines indicate commutativity with an eavesdropper Eve.

Since 3-cycle graphs are chordal, we write down the ENC inequalities over all such subgraphs appearing in the chordal graph in Fig. 4.3:

$$H(A_0|B_0) - H(A_0|E) - H(E|B_0) \leq 0, \tag{4.17}$$
$$H(A_0|E) - H(A_0|B_1) - H(B_1|E) \leq 0, \tag{4.18}$$
$$H(B_1|E) - H(B_1|A_1) - H(A_1|E) \leq 0, \tag{4.19}$$
$$H(A_1|E) - H(A_1|B_0) - H(B_0|E) \leq 0. \tag{4.20}$$

All the above inequalities are always satisfied (because they belong to a chordal graph) and can thus be added to give

$$H_{K_1} - H(E|B_0) - H(B_0|_E) \leq H_{K_1} + 2I(E : B_0) \leq 0, \tag{4.21}$$

where we have used the inequality $-H(B_0|E) - H(E|B_0) \leq 2I(E : B_0)$. For a violation, $H_{K_1} > 0$, the above inequality can never be satisfied, thereby contradicting our original assumption about Eve distributing the correlations according to Eq. (4.16). Therefore, whenever Alice and Bob observe a violation, they can be assured that their outcomes could not have been correlated to any third party. □

Proposition 4.4.1 implies that since the required tripartite probability distribution as given in (4.16) cannot exist when Alice and Bob are violating the inequality, any

strategy by Eve must be of the form

$$P(a,b,e|A_x,B_y,E) = \gamma P_{AB}(a,b|A_x,B_y) + (1-\gamma)P_{AE}(a,e|A_x,E), \tag{4.22}$$

where e is an outcome to a procedure E used by an eavesdropper Eve to guess the bit of Alice, $P_{AB}(a,b|A_x,B_y)$ denotes the probability distribution over the observables A_x and B_y with Alice and Bob and $P_{AE}(a,e|A_x,E)$ represents the probability distribution over the observable A_x with Alice and the procedure E with Eve. The maximal entropic correlations, given by the entropic box (4.8) are distributed between Alice-Bob and Alice-Eve with probability γ and $1-\gamma$, corresponding to $P_{AB}(a,b|A_x,B_y)$ and $P_{AE}(a,e|A_x,E)$ respectively. This way she tries to be correlated with Alice with a probability $1-\gamma$. The above strategy is therefore seen to be the optimal one for Eve, only in the case when Alice and Bob are observing a violation. This point is essential and its importance will be shown when we derive the condition of DI security in Sec. 4.5. However, as we next show, her violation is further bounded by monogamy of entropic non-contextuality inequalities.

Proposition 4.4.2. *A monogamous relationship for a set of observables, X_i corresponding to m non-contextuality scenarios exists if their joint commutation graph can be vertex decomposed into m chordal subgraphs such that all edges appearing in the original m non-contextuality graphs must appear at least once in the decomposition.*

Proof. We prove the above proposition for $n = 4$ and $m = 2$, while providing a mechanism to derive a monogamous relationship for arbitrary values of n and m. A standard monogamous relationship between two entropic non-contextuality scenarios, K_1 and K_2 should be of the form of

$$H_{K_1} + H_{K_2} \leq 0, \tag{4.23}$$

where $H_{K_{1(2)}} \leq 0$ denotes the existence of a joint probability distribution over the n observables. The Eq. (4.23) then physically implies the existence of a joint probability distribution over all the observables appearing in K_1 and K_2.

To that end, each term appearing in Eq. (4.4) corresponds to an edge in the commutativity graph. It follows that to achieve the form of Eq. (4.23) the joint graph of the non-contextuality scenarios must be decomposable into chordal graphs (which admit a joint probability distribution) with the additional feature that all edges of the individual non-contextuality graphs must appear at least once. Missing even one edge would make one of the non-contextuality inequalities incomplete and Eq. (4.23) unachievable.

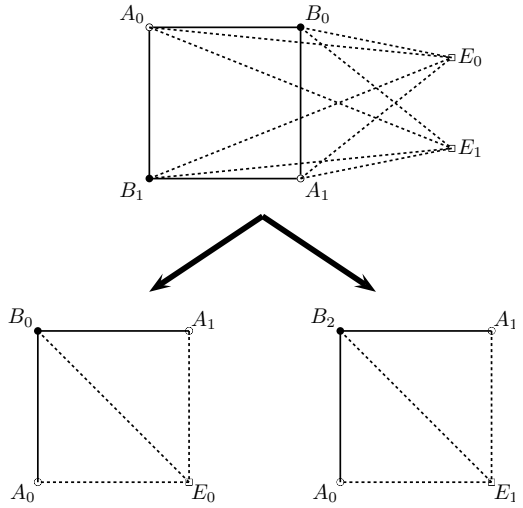

Figure 4.4: The joint commutation graph of Alice-Bob-Eve (top) and its chordal decomposition (below) according to Proposition 4.4.2, where solid lines indicate commutativity between observables of Alice and Bob, while dashed lines indicate commutativity between Alice(bob) and Eve.

Decomposition of the joint graph into chordal graphs enables one to write down the entropic inequalities of all the 3-cycle subgraphs appearing in each chordal graph. Lastly, adding all the entropic inequalities obtained in the aforementioned manner leads to a monogamous relationship between the non-contextuality scenarios.

We now elucidate the proof by deriving a monogamous relationship of the entropic CHSH inequality (4.11) from a graph theoretic perspective which we will use later on, while the mechanism itself is applicable to arbitrary scenarios. Consider the CHSH scenario in which two parties Alice and Bob can perform a measurement of the observables A_0, A_1 and B_0, B_1 respectively. We assume a third party Eve with observables E_0 and E_1, which commute with the observables of Alice and Bob. The scenario is illustrated by a joint graph as shown in Fig. (4.4), where vertices represent observables and edges indicate the commutation relationship. Without loss of generality we assume that Eve would like to violate the entropic CHSH inequality with Alice. The two corresponding Alice-Bob and Alice-Eve entropic CHSH inequalities are,

$$\begin{aligned} H_{K_1} :& H(X_1|X_4) - H(X_1|X_2) \\ & - H(X_2|X_3) - H(X_3|X_4) \leq 0, \end{aligned} \tag{4.24}$$

$$\begin{aligned} H_{K_2} :& H(X_1|X_5) - H(X_1|X_6) \\ & - H(X_6|X_3) - H(X_3|X_5) \leq 0. \end{aligned} \tag{4.25}$$

The joint commutation graph is decomposed into two chordal graphs while keeping the edges appearing in the individual Alice-Bob and Alice-Eve CHSH scenarios intact in the decomposition, as shown in Fig. (4.4). The corresponding ENC inequalities for each 3-cycle graph in every chordal subgraphs are given as,

$$H(X_1|X_5) - H(X_1|X_2) - H(X_2|X_5) \leq 0, \tag{4.26}$$

$$H(X_2|X_5) - H(X_2|X_3) - H(X_3|X_5) \leq 0, \tag{4.27}$$

$$H(X_1|X_4) - H(X_1|X_6) - H(X_6|X_4) \leq 0, \tag{4.28}$$

$$H(X_6|X_4) - H(X_6|X_3) - H(X_3|X_4) \leq 0, \tag{4.29}$$

Being cyclic and chordal, all the above inequalities are a necessary and sufficient condition for a joint probability distribution to exist. Adding the above inequalities and grouping the terms according to H_{K_1} and H_{K_2}, we obtain

$$H_{K_1} + H_{K_2} \leq 0, \tag{4.30}$$

which is the required monogamy relationship. We note that this monogamy relationship was also derived in [79], albeit in a different manner and specifically for the entropic CHSH inequality. The above formalism can be readily generalized to n observables distributed among m parties. □

The derived monogamy relationship (4.30) imposes severe restrictions on the violation of Alice-Eve entropic CHSH inequality. Qualitatively, it is clear that if Alice and Bob share correlations that violate an entropic inequality (4.11), Eve cannot gain much information of Alice's bits by being correlated with her. In subsequent sections we use the above monogamy relationship and its generalization to n observables to provide a detailed quantitative analysis of minimum required correlations between Alice and Bob such that a secure key can be distilled.

4.5 Security

In this section we provide a quantitative analysis of the required minimum correlations between Alice and Bob to achieve secure key distribution. We first analyse the case for entropic CHSH and relate the derived condition for security to violation of Bell-CHSH. In later subsections we generalize the derived condition for even n observables.

Table 4.1: Correlations between Alice and Eve for different measurement settings (horizontal rows) and outcomes (vertical columns)

a, e \ x, z	00	01	10	11
00	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{4}$
01	$\frac{\gamma}{2}$	$\frac{\gamma}{2}$	$\frac{\gamma}{2}$	$\frac{1+\gamma}{4}$
10	$\frac{\gamma}{2}$	$\frac{\gamma}{2}$	$\frac{\gamma}{2}$	$\frac{1+\gamma}{4}$
11	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{4}$

4.5.1 Security from entropic CHSH inequality

We assume that the eavesdropper, Eve, is able to distribute the correlations between Alice, Bob and herself with the help of the no-signalling probability distribution (4.22) as detailed above. The correlations as observed by Eve are given in Table 4.1. These correlations are a classical mixture of the Alice-Eve entropic box and perfect anticorrelations and are given as

$$\begin{aligned} P(a,e|A_x,E_z) = (1-\gamma)P_{AE}(a,e|A_x,E_z) \\ + \gamma P_{C'}(a,e|A_x,E_z), \end{aligned} \tag{4.31}$$

where $P_{C'}(a,e|A_x,E_z) = \frac{1}{4}\left(1+(-1)^{a\oplus b\oplus 1}\right)$ is just a classical box with perfect anticorrelations instead of correlations.

The entropic CHSH inequality, H_{K_2} for Alice-Eve correlations can then be evaluated as

$$H_{K_2} = 3I(A_0:E_0) - I(A_1:E_1) - 2, \tag{4.32}$$

where we have used the fact $I(A_0:E_0) = I(A_0:E_1) = I(A_1:E_0)$ as evaluated from Table 4.1. Therefore, given the correlations as in Table 4.1 and the fact that Alice's input is never known, the best strategy for Eve would be to always input 0 as a setting in her device. This way she can maximize the violation of the inequality (4.32).

Therefore, her violation would be lower bounded as

$$H_{K_2} \geq 2I(A_0 : E_0) - 2. \tag{4.33}$$

From monogamy of entropic CHSH inequality (4.30) we have $H_E + H'_E \leq 0$. Applying this in Eq. (4.33), we get the upper bound on the violation of the inequality between Alice and Bob as

$$H_{K_1} \leq 2 - 2I(A_0 : E_0). \tag{4.34}$$

In order to obtain a positive secure key, it is required that

$$I(A : B) > I(A : E). \tag{4.35}$$

Since the best strategy of Eve dictates using only the measurement setting 0, her mutual correlations with Alice translate to $I(A : E) = I(A_0 : E_0) + I(A_1 : E_0) = 2I(A_0 : E_0)$ which, after substitution in Eq. (4.35) gives

$$H_{K_1} + 2I(A_1 : B_1) + 2 > 2I(A_0 : E_0). \tag{4.36}$$

The intersection of the solutions to the two Eqs. (4.34) and (4.36) defines the region of obtaining a secure quantum key. It is seen that there exists a region of security for

$$H_{K_1} > -I(A_1 : B_1). \tag{4.37}$$

From the above condition it seems that one need not even violate the ENC inequality for DI security. However, as shown above, the strategy of Eve (4.22) is optimal only for the region $H_{K_1} > 0$. For the negative region, she can always distribute a classical box (4.7) being correlated to Alice (Bob) and still gain information on the key. Therefore, the condition which identifies security for the optimal strategy of Eve is found to be a subset of Eq. (4.37), given as

$$H_{K_1} > 0. \tag{4.38}$$

However, we do not completely discard the condition (4.37), which we will use to relate with DI security obtained in the case of Bell-CHSH violation in the following subsection.

4.5.2 Relation with DIQKD using Bell-CHSH

In this subsection we show an unexpected relationship between the correlations offering DIQKD as obtained from Bell-CHSH and those offering DIQKD from ENC as derived above.

Before elucidating the result we provide a qualitative proof. It is important to note that (noisy) correlations between Alice and Bob could arise from various factors including presence of noise in the channel, eavesdropper, misalignment of reference frames, noisy measurements etc. For a DI approach, no aforementioned constraints are put on the channel or devices with Alice and Bob; one is only concerned with the observed correlations between them and not how they arose. Therefore, without loss of generality, the condition (4.37) can be compared with the one derived in [59] by evaluating the basis of measurements which saturate the inequality (4.37) and calculating the Bell CHSH violation for the same. The required measurement basis can be evaluated by using Eq. (4.13) and (4.37), which corresponds to $\theta = 0.50$ rads. The violation of CHSH inequality evaluated for this basis turns out to be equal to 0.83 which is the same as in [59] up to some numerical errors. Therefore, correlations not exhibiting a violation of the entropic CHSH inequality are still secure as they lie in the region of security as dictated from violation of CHSH inequality.

We now provide a quantitative analysis of the same. Before proceeding, it should be noted that the DI correlations as obtained from the negative region of Eq. (4.37) include correlations which are entropically classical and local as well as which are entropically classical and non-local. In order to make a concrete connection with DI correlations obtained from Bell-CHSH, we only consider those correlations following the optimal strategy of Eve (4.22) and declared non-local by Bell-CHSH inequality.

From Eq. (4.22), the correlations as observed by Alice and Bob under the strategy so dictated for Eve are as given in Table 4.2. These correlations are derived in a manner similar to Eq. (4.31). From Eq. (4.37) and Table 4.2, the value of γ for which DI can be achieved is evaluated to be $\gamma = 0.938$. For the same value of γ it is a routine calculation to evaluate the Bell-CHSH violation [59] which is found to be 0.836, which are the same as derived in [58, 59] up to numerical errors. Therefore it is found that the correlations which offer device independence security for entropic inequalities are the same as the ones offering the DI security for Bell-CHSH inequalities. This result is surprising as such a region is not expected a priori. Furthermore, the condition (4.37) singles out all the correlations which will offer DI security, irrespective of the form of non-locality used (standard or information theoretic).

4.6 Conclusion

In this chapter we devised a DIQKD protocol based on entropic correlations, which we term as entropic key distribution (EKD) protocol. Although the protocol is generalized for even n number of observables, we explicitly provided the relevant measurements basis for 4 observables to be chosen by Alice and Bob to maximize their correlations.

Table 4.2: Correlations between Alice and Bob for different measurement settings (horizontal rows) and outcomes (vertical columns) under an optimal strategy of Eve.

a,b \ x,y	00	01	10	11
00	$\frac{\gamma}{2}$	$\frac{\gamma}{2}$	$\frac{\gamma}{2}$	$\frac{\gamma}{4}$
01	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{2}$	$\frac{1}{2} - \frac{\gamma}{4}$
10	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{2}$	$\frac{1-\gamma}{2}$	$\frac{1}{2} - \frac{\gamma}{4}$
11	$\frac{\gamma}{2}$	$\frac{\gamma}{2}$	$\frac{\gamma}{2}$	$\frac{\gamma}{4}$

These correlations correspond to a violation of the ENC inequality and the entire scenario is reminiscent of the CHSH inequality. We then showed that a supraquantum eavesdropper, Eve, limited only by the no-signalling principle cannot be correlated to either Alice or Bob, if their correlations violate an ENC inequality. This lead to the emergence of monogamy relations between Alice, Bob and Eve, which we showed by a graph theoretic analysis. Our strategy to check for the existence and derivation of monogamies using graph theory can be applied to arbitrary scenarios of ENC inequalities. Furthermore, the optimal strategy of Eve is also discussed against which the protocol is shown secure. Using the derived monogamy relations we showed that Eve's optimal information about the key is upper bounded and the key can be deemed secure if Alice and Bob's correlations violate the ENC inequality. From our approach we also identified a set of correlations deemed secure in DI manner to be exactly the ones as derived in [58, 59] necessary for DI security in the case of Bell-CHSH inequality. Unlike DI security based on Bell's inequalities our condition can be easily generalized to even n observables, which we also show. Furthermore, since our EKD protocol requires evaluation of Shannon entropies, it is also possible to implement it using current experimental techniques.

Chapter 5

Role of Bell violation and local filtering in quantum key distribution

5.1 Introduction

Quantum information theory has been instrumental in the development of quantum key distribution (QKD) protocols in which two parties, namely Alice and Bob establish a secret key for secure communication [44, 56, 57, 60, 83]. They are majorly classified in two different classes, namely, prepare and measure and entanglement based.

QKD Protocols in both the classes as mentioned above are proven to be robust against eavesdropping [58, 59, 64, 65, 66] and have been shown to be fundamentally secure as opposed to the classical key distribution protocols.

It has been shown that a violation of a Bell type inequality is necessary for the security of an entanglement based QKD protocol [84, 85], even though the security of the protocol can be shown by comparing the information content of the eavesdropper to the information content of the two involved parties [86]. It is also known that entanglement is necessary but not sufficient to violate a Bell's inequality [87]. From these arguments, a huge class of entangled states is rendered unusable for entanglement based QKD. Furthermore, the question whether Bell violation is also a sufficient condition for the security of QKD is also not definitely settled and has been a matter of debate [58]. Since entanglement is an expensive resource, it is important to characterize such states and explore if it is possible to carry out QKD with states which are entangled but do not violate any Bell's inequalities.

Any Bell type inequality [23, 35] such as the CHSH inequality [10], I_{3322} inequality [88, 89], and the CGLMP inequality [68], characterizes the non-classicality or non-locality of correlations. Due to a lack of analytical results of Bell violation for more

than two measurement on each parties, we consider only the Bell-CHSH inequality in this chapter. However, it is worthwhile to mention that there exist states that do not violate the Bell-CHSH inequality but may violate some other Bell inequality with higher number of measurement settings. A particular example for the same can be found in Ref. [89].

While in the previous chapters we focussed on standard and entropic contextual and Bell inequalities, in this chapter we target the standard Bell-CHSH inequality for QKD. Specifically, we propose a geometrical representation of correlations and relate the Bell-CHSH violation with the secure key rate specifically for the protocols for which the secure key rate is a function of the error rate only. Such a representation allows direct inference of the quantum bit error rate alongwith Bell-CHSH violation. It is extremely helpful in identifying states offering optimal security. Using this representation we also identify a class of states showing Bell-CHSH violation but which do not offer any secure key. These states are therefore unusable for QKD as they lead to a higher error rate. We also show that using local filtering operations some of the states which initially showed no Bell-CHSH violation can be made to provide non-zero secure key rate. Hence, we conclusively prove that Bell-CHSH violation as an initial resource is neither necessary nor sufficient for the security of QKD protocols, thereby proving a conjecture put forward by Acin *et. al.* [58]. To that effect, we propose a modified QKD protocol which uses local filtering to acquire higher secure key rate.

In this chapter we derive our results based only on two assumptions: i) We consider those entanglement based protocols for which the secure key rate is a function of the quantum bit error rate only, and ii) Bell-CHSH violation is necessary to ensure that the correlations shared by the parties are secure. The protocols we consider also encompass one way, two way or n-way communication schemes for entanglement based QKD and are therefore more general.

Various methods to improve the secure key rate have been considered in the literature, many of them focussing on classical post processing schemes like advantage distillation [90]. It has also been shown that there exist bipartite bound entangled states which initially do not violate any known Bell's inequalities, but can be transformed using local operations and classical communications to states from which a secure key can be distilled [91]. However, there also exist states that violate the Bell-CHSH inequality and still cannot be transformed into states useful for QKD, examples of which we provide in this chapter.

Here we use local quantum filtering to alter the secure key rate and Bell-CHSH violation. Local filtering operations allow states to reveal hidden Bell non-locality [92] and can therefore increase the secure key rate. Local filtering is a special class of entanglement distillation and is generally applied on single copies. Moreover, since QKD protocols are typically implemented on photonic systems, single copy operations

prove to be more practical than multicopy operations. Therefore, from an experimental point of view, local filtering is far more accessible than multicopy entanglement distillation [93].

5.2 Background

In this section we describe a general entanglement assisted QKD protocol and discuss many of its features including the quantum bit error rate and secure key rate.

5.2.1 Entanglement assisted QKD protocols

In this chapter, we are interested in only those entanglement assisted QKD protocols in which the secure key rate is a function of quantum bit error rate (QBER). This assumption also encompasses any n-way communication scheme. Here, we define the QBER and the minimum secure key rate r_{min} for the simple entanglement based BB84 protocol.

Consider two parties Alice and Bob who wish to share a secure key. Initially they share a bipartite entangled state ρ. Each of them have a choice of L number of d-outcome mutually unbiased measurement bases (MUBs), where d is the dimension of each of the subsystems. They randomly choose and perform a measurement from the aforementioned set of L observables on their respective subsystems and keep a record of the outcomes. Afterwards, they publicly compare their measurement bases and keep only those outcomes for which their bases matched. The correlations so shared form the raw key. After sharing a raw key, the parties can perform information reconciliation and privacy amplification protocols to share a fully secure key. These protocols utilize classical algorithms and only enhance the raw key. Therefore, if there is no raw key, the protocols will not provide a secure key. Since they are classical in nature we do not consider them in our analysis, but rather focus on the raw key itself.

In the ideal scenario, after basis reconciliation Alice and Bob are left with perfectly identical keys. However, in a pragmatic scenario, imperfections in preparation of the state, its transmission and the subsequent measurement processes can yield differences in their key strings. Therefore, they may be not perfectly correlated. Alice and Bob can estimate the average error in their correlations by calculating the QBER Q after comparing a small portion of their secret key. Formally, the QBER Q for a given state ρ is defined as the average mismatch between the outcomes of Alice and Bob when they perform measurements in the correct basis. If Alice has L number of MUB denoted by $\{|\psi_i^\alpha\rangle\}_{i=1}^d$ (for $1 \leq \alpha \leq L$) which are correlated to Bob's MUB $\{|\phi_j^\alpha\rangle\}_{j=1}^d$, then a perfect correlation between the parties would imply that whenever they perform

measurements in the α-th basis and Alice's outcome is $|\psi_i^\alpha\rangle$ then Bob's outcome must be $|\phi_i^\alpha\rangle$. In a realistic scenario, there can be some probability of observing $|\psi_i^\alpha\rangle$ for Alice's measurement and $\left|\phi_j^\alpha\right\rangle$ for Bob's where $i \neq j$. Hence, the QBER which is an average of all these mismatch probabilities and can be expressed as: [86]

$$Q = \frac{1}{L}\sum_{\alpha=1}^{L}\sum_{i\neq j=1}^{d}\langle\psi_i^\alpha\phi_j^\alpha|\rho|\psi_i^\alpha\phi_j^\alpha\rangle. \tag{5.1}$$

The expression for QBER in Eq. (5.1) holds for any $L \leq d+1$ number of MUBs. For the purpose of this chapter we restrict our analysis to qubits only, i.e., $d = 2$. In this scenario and for the case of two mutually unbiased measurement basis with each party, QBER can be calculated using Eq. (5.1) as

$$\begin{aligned} Q = &\frac{1}{4}\left(2 - \boldsymbol{x}_0^t T \boldsymbol{y}_0 - \boldsymbol{x}_1^t T \boldsymbol{y}_1\right), \\ &\frac{1}{4}\left(2 - |\lambda_1| - |\lambda_2|\right), \end{aligned} \tag{5.2}$$

where $\boldsymbol{x}_i$ and $\boldsymbol{y}_j$ are the Bloch vectors of the measurement basis with Alice and Bob, respectively, and T is the correlation matrix obtained from the two qubit state ρ and λ_1 and λ_2 are the two largest singular values of the matrix T. It should be noted and as is also intuitive that minimization of the QBER will maximize the secure key rate r_{min}.

In a similar fashion, it is possible to analyse the case of $L = 3$, in which both the parties have a choice of three mutually unbiased measurement basis. For this case, the QBER can be calculated as,

$$\begin{aligned} Q &= \frac{1}{6}(3 - \boldsymbol{x}_0^t T \boldsymbol{y}_0 - \boldsymbol{x}_1^t T \boldsymbol{y}_1 - \boldsymbol{x}_2^t T \boldsymbol{y}_2) \\ &= \frac{1}{6}(3 - |\lambda_1| - |\lambda_2| - |\lambda_3|). \end{aligned} \tag{5.3}$$

Due to a lack of complete analytical understanding of Bell inequalities which use more than two measurement basis, we focus our work on $L = 2$ case. This corresponds to the well known Bell-CHSH inequality. The minimum secure key rate r_{min} is defined as the average number of secret bits that can be distilled from each run of the protocol when both the parties peform measurements in the basis as dictated by the protocol. The secure keyrate r_{min} depends on a number of factors including the strategy incorporated by the eavesdropper and the QBER Q. Hence there is no general expression for calculating r_{min} for a given value Q. For some special cases, it is possible to estimate r_{min} and arrive at an expression. As an example, consider the case of symmetric

attacks by Eve (as presented in Ref. [86]) in entanglement assisted protocols for qubits with two measurement settings, the secure key rate is given as [86]

$$r_{min} = 1 + 2(1-Q)\log_2(1-Q) + 2Q\log_2 Q. \tag{5.4}$$

It should be noted that only when $r_{min} > 0$, is it possible to distill a secure key from the correlations between the parties. This condition constraints the maximum QBER to $Q \approx 11\%$ for the symmetric attacks. However, for other protocols it might be more or less than 11%.

From the above it is seen that QBER and the expectation value S of the Bell operator are both functions of the singular values λ_1, λ_2 of the correlation matrix T. Therefore, we now have two separate conditions for the security of a QKD protocol. The first one being $r_{min} > 0$ for a secure key to be distilled while the second dictates that the underlying entangled state must necessarily violate the CHSH inequality.

5.2.2 Local filtering

In this subsection, we present a special class of local quantum operations which we show to be useful for concentrating entanglement and Bell-CHSH correlations in two-qubit systems. These operations are termed as local filtering operations.

Local filtering operations transform a state ρ to ρ', the latter of which has a higher concentration of entanglement and Bell non-local correlations. Consider single-qubit measurements acting locally on a two-qubit system where the measurement operators M_1, M_2 act on the first qubit and N_1, N_2 act on the second qubit. For completeness of measurement outcomes, we have $M_2 = \sqrt{\mathbb{1} - M_1^\dagger M_1}$ and $N_2 = \sqrt{\mathbb{1} - N_1^\dagger N_1}$. The state after measuring M_1 and N_1 on their local subsystems is given by,

$$\rho' = \frac{(M_1 \otimes N_1)\rho(M_1 \otimes N_1)^\dagger}{\text{Tr}((M_1 \otimes N_1)\rho(M_1 \otimes N_1))}. \tag{5.5}$$

The entanglement content, denoted by concurrence, in the state ρ' is related to the entanglement content in ρ as [94, 95],

$$C(\rho') = C(\rho)\frac{|\text{det}(M_1)||\text{det}(N_1)|}{\text{tr}((M_1^\dagger M_1 \otimes N_1^\dagger N_1)\rho)}. \tag{5.6}$$

As can be seen the entanglement content in the latter state can be made to increase if we consider operations with $|\text{det}(M_1)| \neq 0$ and $|\text{det}(N_1)| \neq 0$ and $|\text{det}(M_1)||\text{det}(N_1)| > \text{Tr}((M_1^\dagger M_1 \otimes N_1^\dagger N_1)\rho)$. It should be noted that a higher entanglement content does not necessarily imply higher Bell-CHSH violation. However, it can be shown that for a certain class of states, Bell-CHSH violation can also be made to increase [96] by local

filtering. Specifically, the state ρ can be filtered to a state ρ' which is Bell diagonal or a special form of the 'X' state [33, 92] and subsequently has higher entanglement content and higher Bell non-local correlations.

Following Ref. [92], we briefly illustrate the method to obtain a two-qubit filtered state.

Any valid operations on the state ρ can be seen as a proper orthochronous Lorentz transformations on the Mueller matrix M [Eq. (1.16)] as

$$M' = L_{M_1} M L_{N_1}^T. \tag{5.7}$$

The Lorentz transformations, L_{M_1} and L_{N_1} are given in terms of the measurement operators as:

$$\begin{aligned} L_{M_1} &= \frac{T(M_1 \otimes M_1^*)T^\dagger}{|\text{det}(M_1)|}, \\ L_{N_1} &= \frac{T(N_1 \otimes N_1^*)T^\dagger}{|\text{det}(N_1)|}, \\ \text{with } T &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & i & -i & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}. \end{aligned} \tag{5.8}$$

Further, the Mueller matrix M can be brought to a diagonal or a special form by Lorentz transformations L_1 and L_2 as

$$M = L_1 \Sigma L_2^T, \tag{5.9}$$

where Σ is a diagonal Mueller matrix corresponding to a Bell diagonal state or of the form

$$\Sigma = \begin{pmatrix} a & 0 & 0 & b \\ 0 & d & 0 & 0 \\ 0 & 0 & -d & 0 \\ c & 0 & 0 & a+c-b \end{pmatrix}, \tag{5.10}$$

where a, b, c, d are real numbers. The latter form can be brought close to a Bell diagonal state for $d \neq 0$ by repeated applications of local filtering operations, while $d = 0$ corresponds to a separable initial state [97]. A closed form solution relating Bell violation and local filtering can also be found in Ref. [97].

These optimal local filtering operations applied on the corresponding Mueller matrix can be represented as matrices. These matrices can be constructed by considering its columns as the eigenvectors of MGM^TG and its transposition respectively, where $G = \text{diag}(1, -1, -1, -1)$ is the Minkowski metric. The Mueller matrix M under these optimal Lorentz transformations then transforms as

$$M' = L_1^T G M G L_2. \tag{5.11}$$

Finally, the singular values of the matrix M_{ij}, $i, j \in \{1, 2, 3\}$ are the singular values of the correlation matrix T.

It is to be noted that the set of states corresponding to the non-diagonal Mueller matrix Σ is of measure zero and thus has almost zero probability of occurrence. In some scenarios these states can be brought to a Bell diagonal form with higher entanglement content and Bell-CHSH violation.

It is worth noting that local filtering operations for two qubit systems are a special case of entanglement distillation [94, 95]. This is the case when the aforementioned local operations are performed on single copies of the quantum state. In contrast, distillation requires multiple copies of the quantum state. In the present work we however, restrict the access of the interested parties to single copies. Under this paradigm we then calculate the quantum bit error rate after local filtering.

5.3 Results

In this section, we develop a geometrical representation of quantum correlations to study the Bell-CHSH violation and the QBER for arbitrary two-qubit states. We achieve this task under the following assumptions:

1. We consider only those entanglement based protocols for which the secure key rate is a function of QBER only and,

2. Bell-CHSH violation is necessary for security.

Following only these two assumptions, we apply our representation of quantum correlations to explicitly identify states are optimally secure and states which are not for the purpose of QKD. This identification is done for a fixed value of Bell-CHSH violation. Our geometrical representation offers a useful visualization of arbitrary two-qubit states from the viewpoint of QKD. We then formulate a modified QKD protocol which involves local filtering to improve the key rate. Finally, we conclude by providing explicit examples of two qubit states which initially do not exhibit any Bell-CHSH violation but can be transformed to states with non-zero secure key rate after local filtering.

5.3.1 Geometrical representation of correlations

As detailed in Sec. 1.1.5, all two-qubit states can be parameterized by the two largest singular values of the real correlation matrix T. This is true if the scenario of interest is Bell-CHSH inequality. For a bonafide quantum state all the singular values of the T matrix must satisfy $|\lambda_i| \leq 1$ and $\sum_i \lambda_i^2 \leq 3$. The region outside these constraints

correspond to unphysical states and are not valid density matrices. For ease of calculations we only consider the region $0 \leq \lambda_1 \leq 1$ and $0 \leq \lambda_2 \leq 1$ as all the arguments presented below apply equally well to the other valid regions.

A geometrical representation of all two-qubit states parameterized by their two largest singular values of the correlation matrix T is depicted in Fig. 5.1. In this representation all physical states are represented by shaded regions while the unshaded region corresponds to unphysical states. As can be seen all the physical states with a fixed value of S of the expectation value of the CHSH operator lie on the circular arc $\lambda_1^2 + \lambda_2^2 = S^2/4$. Therefore, the set of all physical states that all show a violation of the Bell-CHSH inequality lie outside the disc of unit radius $\lambda_1^2 + \lambda_2^2 \leq 1$, as is evident from Eq. (1.19). Meanwhile the set of physical states lying outside this region do not show a violation. Thus, for a given physical state its distance from the origin quantifies the Bell-CHSH correlation and if this distance is above 1 the state is seen to violate the Bell-CHSH inequality.

In this geometric representation, the QBER Q (5.2) is represented by straight lines with slope -1, i.e, $\lambda_1 + \lambda_2 = m$ (Fig. 5.1), where m is the y-intercept. These states offer the same $Q = \frac{1}{4}(2 - m)$. Increasing values of m for the straight lines corresponds to a decreasing QBER.

5.3.2 Characterization of states based on the geometrical representation

Using the geometrical representation of quantum correlations as described above it is possible to identify states which violate the Bell-CHSH inequality, but still cannot be used to distill a secure key rate. This technique of recognizing states which are useless for QKD, is more strict than the one identified earlier [86]. Our representation also enables identification of a set of states most suitable for experimentally implementing entanglement assisted QKD protocols with a fixed violation of the Bell-CHSH inequality.

As is evident from Fig. 5.1, the set of states having the same Bell-CHSH value S do not necessarily share the same QBER Q. Therefore, for the same Bell-CHSH violation, states might not share the same secure key rate r_{min}. Since quantum entanglement is an expensive resource to produce, the variation in the QBER for the same value of Bell-CHSH violation S indicates that some states are more suitable for performing QKD than others. This further implies that Bell-CHSH violation alone cannot provide a full characterization of the security of an entanglement assisted QKD protocol.

It should be noted that all states saturating the Bell-CHSH bound lie on the circle $\lambda_1^2 + \lambda_2^2 = 1$. However, as is also noted in Sec. 5.3.1 all of these states do not share the same QBER Q. The set of states offering the least Q for a given value of S lie

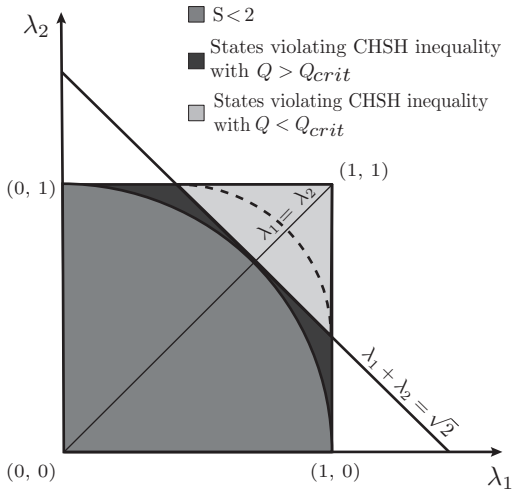

Figure 5.1: A geometrical representation of the Bell-CHSH inequality and the QBER Q parameterized by λ_1 and λ_2. The dark grey region corresponds to states which violate the Bell-CHSH inequality but offer $Q > Q_{crit}$. These states are therefore unusable for QKD. Only the states lying in the light grey region offer a secure key rate while also violating the Bell-CHSH inequality.

on the line which is tangent to the circle of radius $S/2$ satisfying $\lambda_1 = \lambda_2 = S/2\sqrt{2}$. Therefore the set of local states saturating the Bell-CHSH inequality and offering the least QBER correspond to the point $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$ (Fig. 5.1). These states offer no security for QKD as we have assumed that the Bell-CHSH violation is necessary for the same. We define the QBER at for the set of states at this point as the critical error rate given by $Q_{\text{crit}} = \frac{1}{4}\left(2 - \sqrt{2}\right) \approx 0.14$, which is the maximum allowed QBER for any QKD protocol (based on our assumptions) to be secure, irrespective of the type of attacks by an eavesdropper. All the state on the line $\lambda_1 + \lambda_2 = \sqrt{2}$ have the same critical error rate (Fig. 5.1). Therefore, all valid quantum states lying below this line posses a higher QBER and therefore can not be used for QKD. To summarize, all the states above $\lambda_1^2 + \lambda_2^2 = 1$ violate the Bell-CHSH inequality and all the states below $\lambda_1 + \lambda_2 = \sqrt{2}$ have QBER more than Q_{crit}. Therefore they are unusable for QKD. The region of intersection between these two regions contain states which are useless for QKD, even though they are Bell non-local.

The line corresponding to the critical QBER, $\lambda_1 + \lambda_2 = \sqrt{2}$ provides the theoretically maximum tolerable QBER for carrying out secure QKD using Bell-CHSH violation as a necessary assumption. It may be the case that for a particular QKD protocol Q_{crit} is smaller than the one we obtained. As an example, Q_{crit} in the protocol presented in [86] is $Q'_{crit} = 0.11$ which is smaller than the theoretical critical value calculated from our representation. The reason for this is because Q'_{crit} is obtained from a particular form of r_{min} which implicitly depends on the attacks and strategies chosen by the eavesdropper and the particular communication scheme chosen by Alice and Bob. For the huge class of attacks detailed in Ref. [86], r_{min} takes on the form as given in Eq. (5.4). The value of $Q'_{crit} = 0.11$ has also been shown to be optimal under two way communication schemes [58, 98]. However, it is possible that there might exist attacks that may not result in the aforementioned function of secure key rate. Furthermore, by employing n-way communication schemes, the tolerable QBER may also be improved. For these schemes the form for secure key rate is also different than the ones obtained in [86]. However, our results are more general as we do not make any assumptions on the various forms of attacks and strategies by the eavesdropper or any communication scheme, but rather that the correlations with Alice and Bob violate the CHSH inequality.

In order to perform QKD protocols, it is necessary to transmit the quantum systems through channels which might be noisy. The noise can then affect the state of the quantum systems. Therefore, it is not always possible to achieve the quantum maximum of the Bell-CHSH inequality. In these cases, it is desirable to identify states most suitable for QKD for a particular value of Bell-CHSH violation. Furthermore, these states should also have the property of offering the least QBER for a fixed violation. As detailed in Sec. 5.3.1, these set of states are identified with the points

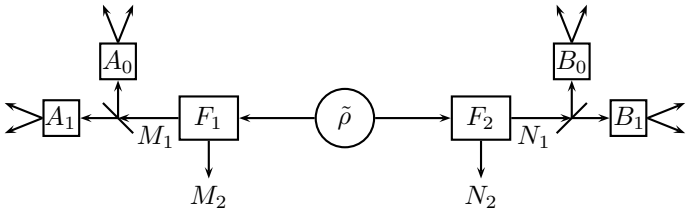

Figure 5.2: A schematic diagram to implement the modified QKD protocol using local filtering operations. Each party shares an initial entangled state $\tilde{\rho}$ on which they both apply local filters denoted by F_1 and F_2. Using classical communication, the parties discard the events when any of the parties observed the outcome M_2 or N_2. Only when both the parties observe M_1 and N_1 do they proceed to perform the measurements A_0, A_1 and B_0, B_1 as dictated by the protocol.

$|\lambda_1| = |\lambda_2| > 1/\sqrt{2}$.

In a non-ideal situation for QKD, the two parties Alice and Bob may share states violating the Bell-CHSH inequality but with an error rate higher than Q_{crit}. It is then desirable to transform these states such that the QBER is reduced below the critical value so that a secure key can be distilled. Since, QKD is carried out between remote locations, such transformations will necessarily have to be local operations performed by Alice and Bob. However, it is known that local operations in themselves cannot increase the Bell-CHSH violation unless there is some post-selection performed by the parties.

5.3.3 QKD protocol using local filtering operations

In a modified version of entanglement assisted QKD, it is assumed that a source is responsible for generating pairs of qubits in maximally entangled states. These states are tranmsitted to Alice and Bob through a channel. It may be the case that the source is in the lab of one of the parties, and the second subsystem is transmitted to the other party via a quatum channel. This does not change the analysis which we are going to present below. Due to various noise factors in the quantum channel and a possible presence of an eavesdropper, the state received by Alice and Bob is generally a mixed state $\tilde{\rho}$, which can be estimated by performing a full state tomography before beginning the actual QKD protocol. Therefore, we naturally begin our protocol by assuming that Alice and Bob share entangled pairs of qubits in the states $\tilde{\rho}$ with Bell-CHSH value S. In order to increase the Bell-CHSH violation and the secure key rate the parties perform local filtering operations. Let M_1 and N_1 be the optimal filtering operators for concentrating entanglement in the state $\tilde{\rho}$ where $M_2 = \sqrt{\mathbb{1} - M_1^\dagger M_1}$ and $N_2 = \sqrt{\mathbb{1} - N_1^\dagger N_1}$

(as described in 5.2.2). $\{A_0, A_1\}$ and $\{B_0, B_1\}$ are the dichotomic observables in Alice and Bob's lab, respectively. The modified protocol consists of the following steps:

1. Alice and Bob perform local operations using $\{M_i\}$ and $\{N_j\}$ measurement settings followed by the measurement of $\{A_0, A_1\}$ and $\{B_0, B_1\}$.

2. Alice and Bob announce the outcome of the measurement in $\{M_i\}$ and $\{N_j\}$ measurement settings and the choice of the measurement operators $\{A_0, A_1\}$ and $\{B_0, B_1\}$ for each of the qubit pair.

3. They consider only the qubit pairs for which M_1 and N_1 coincided, i.e., the pairs for which local filtering was successful. Then they reconcile their measurement basis $\{A_0, A_1\}$ and $\{B_0, B_1\}$ and discard the qubits for which the measurement was performed in different bases.

Since, generally QKD protocols are implemented on photonic systems any measurement tends to demolish the state. In this case local filtering followed by the measurements in $\{A_0, A_1\}$ and $\{B_0, B_1\}$ basis can be implemented by post-selection. In Fig. 5.2 we outline of the modified QKD protocol using local filtering operations. Our modified QKD protocol as presented above relies on the fact that it is possible to successfully filter an ensemble of two qubit partially entangled states into a smaller ensemble with higher entanglement content. The states with enhanced entanglement are then used for QKD while the other states are discarded. By using this process it is possible to transform states useless for QKD into those which are useful for QKD with the probability of success in the filtering process being $P_{\text{succ}} = \text{Tr}[(M_1 \otimes N_1)\rho(M_1^\dagger \otimes N_1^\dagger)]$.

5.3.4 Example of states that do not violate Bell-CHSH inequality but can be used for QKD

We now illustrate explicitly some examples of states where filtering process is useful in enhancing the key rate. We begin with the following class of pure two-qubit states:

$$|\psi\rangle = \alpha_1|00\rangle + \alpha_2|11\rangle + \alpha_3|01\rangle, \tag{5.12}$$

where it is assumed that $\alpha_i \in \mathcal{R}$ and $\alpha_1^2+\alpha_2^2+\alpha_3^2 = 1$ and $\alpha_1 \leq \alpha_2 \leq \alpha_3$. Furthermore, it is to be noted that this example of a set of pure state is to be treated as a theoretical exercise rather than occuring in a physical experiment. The state $|\psi\rangle$ is maximally entangled if and only if $\alpha_1^2 = \alpha_2^2 = \frac{1}{2}$ and The Bell-CHSH violation for the state can be calculated readily using the methods described above,

$$S = 2\sqrt{1 + 4\alpha_1^2\alpha_2^2}, \tag{5.13}$$

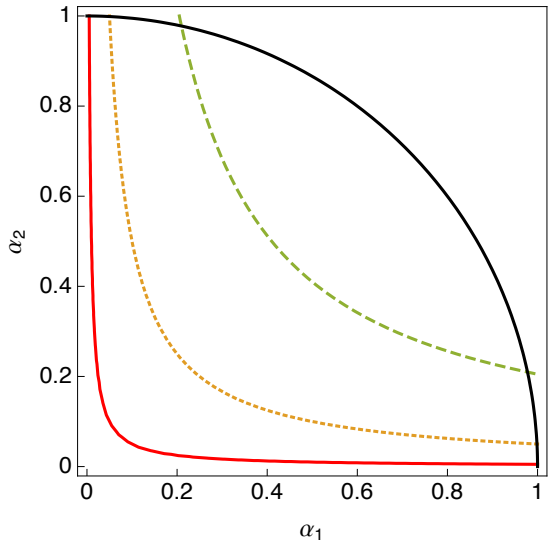

Figure 5.3: Contour plot of $\lambda_1 + \lambda_2$ as a function of α_1 and α_2 with $\lambda_1 + \lambda_2 = 1.01$ (Red solid), $\lambda_1 + \lambda_2 = 1.1$ (Yellow dashed), $\lambda_1 + \lambda_2 = 1.41$ (Green large dashed), while the Black solid line is the boundary for the set of all physical states and corresponds to $\alpha_1^2 + \alpha_2^2 = 1$. For the purpose of QKD it is required that $\lambda_1 + \lambda_2 > 1.41 \sim \sqrt{2}$, which identifies a huge set of states in the parameter space of α_1 and α_2 to be useless for QKD.

where $\lambda_1^2 + \lambda_2^2 = 1 + 4\alpha_1^2\alpha_2^2$ and the error rate to be

$$Q = \frac{1}{4}\left(1 - 2|\alpha_1||\alpha_2|\right), \tag{5.14}$$

where $\lambda_1 + \lambda_2 = 1 + 2|\alpha_1||\alpha_2|$.

We plot contours of $\lambda_1 + \lambda_2$ in Fig. 5.3 for this particular class of pure states. From Fig. 5.3 it can be inferred that there exist a huge set of states which have $Q > Q_{crit}$. As an example, consider the state given by $\alpha_1 = 0.1$ and $\alpha_2 = 0.2$, we have

$$\begin{aligned} \lambda_1 + \lambda_2 &= 1.0400 < \sqrt{2}, \\ \lambda_1^2 + \lambda_2^2 &= 1.0008, \end{aligned} \tag{5.15}$$

which implies that the state shows very little Bell-CHSH violation and has error rate higher than the critical value. It is well known that all two qubit entangled states are distillable an in principle, it is possible to perform entanglement distillation (single-copy or multi-copy) and distil pure two qubit Bell states. In this case the entanglement of formation is the same as distillable entanglement which reads,

$$E(\psi) = -\text{Tr}(\rho_A \log_2 \rho_A) = 0.005, \tag{5.16}$$

where ρ_A is the reduced state of Alice. This gives us a qualitative indication that the state can be used for QKD. However, the method to harness its usefulness remains to be seen.

In order to extract some usefulness from these states, the parties perform local filtering operations. Since in general the underlying systems are optical in nature for the purpose of QKD, it is not clear how multicopy entanglement distillation will be performed. To that end we focus on local filtering, which is a special case of multicopy entanglement distillation dealing only with single copies. After performing local filtering operations, the state $|\psi\rangle$ can be brought into a Bell-diagonal form with the following properties (see Sec. 5.2.2),

$$\begin{aligned} \lambda_1' + \lambda_2' &= 1.7354 > \sqrt{2}, \\ \lambda_1'^2 + \lambda_2'^2 &= 1.2271, \end{aligned} \tag{5.17}$$

where λ_i' are the singular values of the correlation matrix for the state transformed after local filtering.

The above properties state that the filtered state has a higher Bell-CHSH violation and lower QBER than the critical error rate. Therefore, the states (5.12) belonging to the region where Bell-CHSH violation is observed but having $Q > Q_{crit}$ can be filtered to the region where a higher Bell-CHSH violation is observed alongwith $Q < Q_{crit}$. The secure keyrate r of the protocol with these states can be calculated and turns out to be

$$\begin{aligned} r &= P_{\text{succ}} r_{min} \\ &= 0.2565 \text{ bits}, \end{aligned} \tag{5.18}$$

where $P_{\text{succ}} = 0.8638$ is the probability of the successful local filtering and $r_{min} = 0.2972$ bits is the secure bit rate after successful filtering.

It should be noted that any noise acting on the initial state will always yield a mixed state. The aforementioned example might serve as a theoretical exercise to show that pure entangled states can also be filtered locally to obtain higher Bell violation. However, we analyse the properties of the states transformed from Eq. (5.12) under the action of white noise.

We now present a family of mixed states which might occur in some physical realisation of entanglement assisted QKD protocols. These states do not show any Bell-CHSH violation; however, upon local filtering it is possible to distill some non-zero secure key rate from them. Consider the class of states with a density operator given by

$$\begin{aligned} \rho = \frac{1}{4} [\mathbb{1} \otimes \mathbb{1} + \lambda(\alpha^2 - \beta^2)(\sigma_z \otimes \mathbb{1} - \mathbb{1} \otimes \sigma_z) \\ + (1 - 2\lambda)\sigma_z \otimes \sigma_z - 2\lambda\alpha\beta(\sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y)], \end{aligned} \tag{5.19}$$

where $\alpha, \beta \in \mathcal{R}$, $\alpha^2 + \beta^2 = 1$ and $0 < \lambda \leq 1$. These states have been studied extensively under local filtering operations [96]. The behaviour of these states for a fixed value of Bell-CHSH violation and error rate is as plotted in Fig. 5.4. The dark grey region depicts the set of states which can filtered to states which can violate the Bell-CHSH inequality and have $Q < Q_{crit}$. The contour corresponding to Q_{crit} given by $\lambda_1 + \lambda_2 = \sqrt{2}$ is given by the black solid line in Fig. 5.4 and it is seen that there exist states which violate Bell-CHSH inequality and still have $Q > Q_{crit}$. However, these states can also be filtered. As an example consider the state ρ with $\alpha = 0.9$, $\beta = 0.4538$ and $\lambda = 0.85$, with the following properties,

$$\begin{aligned} \lambda_1^2 + \lambda_2^2 &= 0.9347, \\ \lambda_1 + \lambda_2 &= 1.3669. \end{aligned} \tag{5.20}$$

This is an example of a state that does not violate Bell-CHSH inequality and is therefore useless for QKD. The distillable entanglement from this state turns out to be

$$\begin{aligned} E(C(\rho)) &= h\left(\frac{1+\sqrt{1-C^2}}{2}\right) \\ &= 0.3722, \end{aligned} \tag{5.21}$$

where C is the concurrence of the quantum state and $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy. This again states that the state ρ considered above can provide some secure key.

After an application of optimal local filtering operations as detailed above, we get the state ρ' with the following properties:

$$\begin{aligned} \lambda_1'^2 + \lambda_2'^2 &= 1.3329, \\ \lambda_1' + \lambda_2' &= 1.6327. \end{aligned} \tag{5.22}$$

The resultant state ρ' violates the Bell-CHSH inequality with $Q < Q_{crit}$, indicating that it is now a useful state for QKD. Consequently, the keyrate r for the transformed state can be calculated as

$$\begin{aligned} r &= P_{\text{succ}} r_{min} \\ &= 0.091 \text{ bits}, \end{aligned} \tag{5.23}$$

where $P_{\text{succ}} = 0.799$ and $r_{min} = 0.110$ bits.

It should also be noted that at the level of single-copy distillation, the local filtering operations considered above have been shown to be optimal for concentrating entanglement and Bell non-locality [92]. Therefore the key rates obtained after applying local filtering, are the best that can be achieved, given access to individual copies only for the entanglement based QKD protocol.

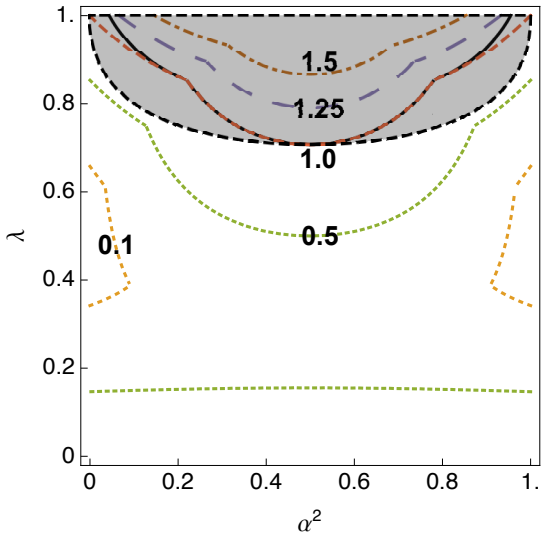

Figure 5.4: Contour plot of states with parameters α and λ as given in Eq. (5.19) with varying values of $\lambda_1^2 + \lambda_2^2$. In order to exhibit Bell-CHSH violation it is required that $\lambda_1^2 + \lambda_2^2 > 1$ (Red dashed). For the purpose of QKD it is required that $\lambda_1 + \lambda_2 > \sqrt{2}$ (Black solid). All states lying below this contour exhibit a higher error rate than Q_{crit} and it can be seen that some of them still exhibit Bell-CHSH violation. The set of useless states that can be made useful by local filtering is given by the region in grey.

Further, according to [92], Bell-diagonal states cannot be filtered further. From Fig. 5.1 it can be easily seen that there exist such Bell diagonal states which exhibit Bell-CHSH violation, having $Q > Q_{crit}$ and which cannot be filtered. These states remain useless for QKD even after filtering, thereby indicating that Bell-CHSH violation is not a sufficient condition either.

5.4 Conclusion

We develop a geometrical representation for two-qubit correlations to quantitatively analyse the relationship between the secure key rate of a QKD protocol and the violation of the Bell-CHSH inequality. The usefulness of this geometrical representation is demonstrated by showing that states sharing the same non-local correlations do not necessarily share the same secure key rate. This leads to an important conclusion that some states are more apt for performing QKD efficiently than others, even when they share the same non-local correlations.

For fixed (non-maximal) Bell-CHSH violation the states that are optimally suited for performing QKD are located, which can be useful when Alice and Bob share a non-maximally entangled state. We use the threshold error rate requirement for security to identify a class of states which cannot be used for QKD, even though they exhibit a violation of the Bell-CHSH inequality. This is an improvement over a previous result and has profound experimental implications to develop QKD protocols with non-maximal violation of Bell-CHSH inequality. Such states which are deemed useless for QKD can be seen as a result of the specificity of the protocol considered or because of errors arising due to preparation, transmission or measurements. To harness the entanglement present in states that do not violate Bell-CHSH inequality we employed local filtering operations and found that the performance of such states can be greatly improved in terms of providing key rate for QKD. The local filtering operations considered is a special subclass of entanglement distillation dealing with single copies. Under the paradigm of single copy distillation not all entangled states can provide a secure key as compared to multicopy distillation in which all two qubit entangled states can be used to distill some secure key. However, multicopy distillation is harder to achieve experimentally than local filtering. Further, the protocol for local filtering described has been shown to be optimal in the case of single copies [92] and the secure key rate obtained under them is the best that can be achieved. We explicitly provided examples when the original state exhibits Bell-CHSH violation but has $Q > Q_{crit}$ and states which do not violate the Bell-CHSH inequality. It is seen that in both cases local filtering offers improvement in secure key rate. Our work paves the way for efficient experimental realization of QKD protocols where Bell-CHSH violation is a necessary resource.

Chapter 6

Non-paradoxical ABL probabilities give no contextual advantage

6.1 Introduction

Aharonov, Bergmann, and Lebowitz (ABL), in their seminal work on the time symmetry in successive quantum measurements [99], introduced a *retrodiction* formula for assigning probabilities to outcomes of hypothetical measurements on a pre-and post-selected (PPS) ensemble at some intermediate time. The counterfactual probability assignments using ABL formula has led to various counter-intuitive and apparently paradoxical results [100, 101, 102, 103] known as pre-and post-selection (PPS) paradoxes. The strong connection of ABL formula with weak values has also enabled its proponents to claim experimental validation of these paradoxes [104, 105, 106, 107, 108].

Contrary to the Born rule, probabilities assigned by ABL formula cannot be determined by only the specification of projectors associated with the measurement outcomes, they rather also depend on other details of the observable being measured. This sort of context dependency of measurements led Albert, Aharonov, and D'Amato [109] to draw connection between PPS paradoxes and contextuality: since the probabilities assigned to measurement outcomes are explicitly context dependent, there is no motivation to consider a non-contextual hidden variable theory as a realistic extension of operational quantum theory. Nevertheless, this reasoning has been disputed based on the fact that Bell-type correlations can be simulated using post-selections in local hidden variable theories [110]. Therefore, the mere presence of context dependent elements in ABL formula is not sufficient to prove Bell-Kochen-Specker (BKS) theorem [1, 26]. It is therefore necessary to dive deeper in order to establish a valid connection between contextuality and ABL retrodiction formula.

Mermin [111] showed the existence of a strong connection between the two by illustrating how measurements used in a proof of BKS theorem can give birth to unsolvable PPS paradoxes indicating a kind of impossibility of non-contextual hidden variable theories. Leifer and Spekkens [11] later logically showed the converse: for every PPS paradox with a scenario involving non-orthogonal pre-and post-selection states, there exists an associated proof of BKS theorem. Their proof is based on the fact that ABL probability assignments of certain sets of projectors in a variant of 3-box paradox violate algebraic constraints dictated by classical probability theory. Another important contribution in this direction was recently made by establishing a connection between anomalous weak values and contextuality where it has been suggested that anomalous weak values can be taken as proofs of contextuality [112, 113].

So far the studies in this avenue of research have been focused on providing logical proofs of contextuality invoking only the paradoxical nature of ABL probability assignments. Therefore, it is natural to ask here whether there is any contextual advantage of non-paradoxical assignments of ABL probabilities, where any ontic model that can exhibit a violation of a contextual inequality is defined to offer a contextual advantage. In this chapter, by analysing the KCBS [6] scenario for a statistical proof of contextuality with ABL formula, we show that non-paradoxical ABL probability assignments give no contextual advantage. Furthermore, we demonstrate that non-paradoxical sector of ABL probabilities of KCBS projectors gives contextual advantage only if the post-selection is lifted. Our result opens serious questions about the ABL-contextuality connections that have been advocated by previous authors: is this connection merely an illusion created by post-selection just like the detection efficiency loophole in Bell non-locality tests? Since non-paradoxical sector of ABL probabilities can be modelled with a non-contextual hidden variable theory, can ABL retrodiction be considered a valid description of pre-and post-selected quantum systems at all?

In this chapter we first discuss PPS scenarios and the ABL probability rule in brief and then use the same to derive (non-)contextual bounds on the KCBS scenario.

6.2 Pre- and post-selected scenarios

A pre- and post-selection scenario deals with statistical assignment of probabilities to the outcomes of an observable A when the system is selected to be in the state $|\psi\rangle$ prior to measuring the observable and in the state $|\phi\rangle$ after the measurement has occurred. This selection of states is known as pre- and post-selection respectively. These selections can be achieved by performing a projective measurement $\{|\psi\rangle\langle\psi|, \mathbb{1}-|\psi\rangle\langle\psi|\}$ on the initial state of system (which can be chosen arbitrarily depending on the scenario) and selecting only the outcomes corresponding to $|\psi\rangle\langle\psi|$. Similarly for post-selection

one can perform a projective measurement of $\{|\phi\rangle\langle\phi|, \mathbb{1} - |\phi\rangle\langle\phi|\}$ where outcomes corresponding to $|\phi\rangle\langle\phi|$ are selected. The way the assignment of probabilities to the outcomes of observable A is made leads to two entirely different scenarios.

We describe the two cases below. In the first case, the observable A is actually measured after performing a pre-selection. Post selection is then performed on the state after the measurement of observable A. In this case there are a total of three different sequential measurements being performed. This case is known as non-counterfactual assignment of probability distribution.

In the second case, the observable A is not actually measured, but rather a probability distribution over its outcomes is assigned counterfactually depending on the PPS states. This case is known as counterfactual assignment of probabilities to different possible outcomes of A. For both the case, the rule to evaluate the probability distribution remains the same and is given as,

$$\zeta_i = \frac{|\langle\phi|\Pi_i|\psi\rangle|^2}{\sum_j |\langle\phi|\Pi_j|\psi\rangle|^2}, \tag{6.1}$$

where $A = \sum_i p_i \Pi_i$. This rule is eponymously known as the ABL rule and is the same for both the aforementioned cases. However, the interpretation for both the cases is entirely different and leads to some interesting results, especially when linked to counterfactual assignments of projectors in the KCBS scenario.

6.3 Results

In this section we apply the ABL rule to counterfactually assign probabilities to the observables appearing in an operational version of the KCBS scenario. We then analyse the non-contextual and quantum mechanical test of the same.

An operational version of the KCBS scenario consists of 5 tests e_i, $i \in \{0, 1, 2, 3, 4\}$. A test is an experiment which yields some statistics for a given preparation. These tests are assumed to be cyclically exclusive, i.e.,

$$P(e_i) + P(e_{i\oplus 1}) \leq 1, \tag{6.2}$$

where $i \oplus 1$ is taken modulo 5. The entire scenario can be represented on an exclusivity graph, whose vertices correspond to tests and two vertices are connected by an edge if they are exclusive as given in Fig. 1.1. This scenario is capable of revealing quantum contextuality if the following inequality is violated as shown in Eq. 1.5,

$$\mathcal{K} := \sum_{i=0} P(e_i) \leq 2, \tag{6.3}$$

where the underlying ontic probability distributions, $P(e_i)$ are assumed to be non-contextual. For a more detailed discussion on this we refer the reader to Sec. 1.1.2. It is to be noted that this construction of KCBS inequality explicitly refers to the exclusivity conditions. Therefore any statistical verification of the same must necessarily also obey the aforementioned conditions.

A valid construction of the KCBS scenario for the quantum case is as follows. Consider 5 different projective value measurements (PVMs), $\mathcal{M}_i := \{\Pi_i, \mathbb{1} - \Pi_i\}$, $i \in \{0, 1, 2, 3, 4\}$, where $P(\Pi_i = 1)$ denotes the probability of obtaining the outcome Π_i in measurement $\mathcal{M}_i$ and $\text{Tr}[\Pi_i \Pi_{i\oplus 1}] = 0$. Each projector corresponds to a test in the KCBS scenario and cyclic orthogonality ensures the required exclusivity conditions given in Eqn. (6.2). The maximum value of the KCBS inequality (6.3) for the aforementioned settings and a state $|\psi\rangle$ (1.9) is

$$\text{Max}(\mathcal{K}) := \text{Max}\left(\sum_{i=0} P(\Pi_i = 1)\right) = \sqrt{5}, \tag{6.4}$$

which is greater than the non-contextual bound as observed above. This is an indication of contextual advantage of quantum probability distributions. It is to be noted that any valid construction of the KCBS scenario in any formalism must necessarily ensure the exclusivity conditions (6.2).

Any operational signature of (non-)contextuality from the KCBS inequality must necessarily satisfy the aforementioned exclusivity conditions. A noncontextual ontological model assigns an apriori probability to each of the projectors denoted by a response function $\xi_i(\lambda)$ respectively, with λ as an ontic variable, such that $\xi_i(\lambda) \in [0, 1]$ and $\int_\lambda d\lambda \xi_i(\lambda)\xi_{i\oplus 1}(\lambda) = 0$. The latter condition follows from orthogonality of projectors and together with outcome determinism for PVMs [7] implies at most one of $\xi_i(\lambda)$ or $\xi_{i\oplus 1}$ can take on the value 1 and Eqn. (6.3) subsequently follows. Furthermore, the exclusivity conditions

$$\xi_i(\lambda) + \xi_{i\oplus 1}(\lambda) \leq 1 \quad \forall i, \tag{6.5}$$

are still satisfied in a noncontextual ontological model. On the other hand by using carefully constructed PVMs the KCBS inequality can be maximized to the value $\text{max}(\mathcal{K}) = \sqrt{5}$, thereby indicating a contextual advantage.

The foremost requirement to check whether the ABL formalism offers any contextual advantage is to setup the KCBS scenario with the proper exclusivity conditions given in Eqn. (6.2) by assigning a probability distribution ζ_i to the projectors under a pre and post-selection scenario. We choose the pre and post-selected states as $|\psi\rangle$ and $|\phi\rangle$ respectively to assign a probability distribution to the projector Π_i according to the ABL rule as

$$\zeta_i = \frac{|\langle\phi|\Pi_i|\psi\rangle|^2}{|\langle\phi|\Pi_i|\psi\rangle|^2 + |\langle\phi|(\mathbb{1} - \Pi_i)|\psi\rangle|^2}, \tag{6.6}$$

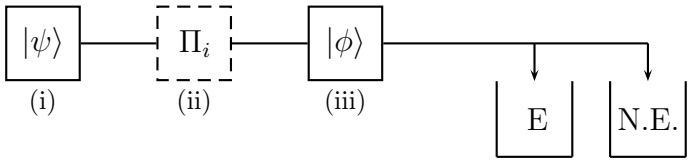

Figure 6.1: A schematic diagram for evaluating the KCBS inequality using the ABL rule. In the figure (i) denotes a pre-selection of state $|\psi\rangle$, (ii) denotes a counterfactual assignment of projectors Π_i, (iii) denotes a post-selection of state $|\phi\rangle$. After post-selection, the states are further segregated into ones which obey exclusivity conditions (E) and ones which do not (N.E.). The KCBS inequality is tested on the states segregated into E.

where we have assumed the measurement to be of the form $\{\Pi_i, \mathbb{1} - \Pi_i\}$.

We would like to note here that this probability distribution is "counterfactually assigned" rather than actually performing the measurement. This reasoning is crucial to the analysis. A non-counterfactual assignment of this probability distribution to the event e_i does not make sense when the question we are interested in is whether such a distribution exists "prior" to performing an actual measurement. Furthermore, the non-counterfactual assignment does not lead to any non-trivial results. Therefore, we are only interested in the case when the ABL rule is used to assign probability distributions counterfactually, i.e., the projective measurement is not actually performed and the pre- and post-selected states are assumed to provide a complete description for any observable.

By careful selection of a pre and post-selected state, such counterfactual assignments can lead to paradoxical situations in which both Π_i and $\Pi_{i\oplus 1}$ are assigned the probability 1 leading to $\zeta_i + \zeta_{i\oplus 1} > 1$, which is a direct violation of the required exclusivity conditions (6.2).As mentioned above such probability distributions do not fall under the paradigm of KCBS scenario and have to be excluded. By imposing exclusivity conditions we are removing all such paradoxes that may arise. We term the resultant ABL rule to calculate probabilities as non-paradoxical ABL probabilities.

We now propose the following setup to test the KCBS inequality using the ABL formalism. Without loss of generality we assume a pre-selected state $|\psi\rangle$ as

$$|\psi\rangle = (0, 0, 1)^T, \tag{6.7}$$

and a post-selected state as

$$|\phi\rangle = (\cos\theta, \sin\theta\cos\phi, \sin\theta\sin\phi)^T, \tag{6.8}$$

where $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi]$. The projectors $\Pi_i = |v_i\rangle\langle v_i|$ are of the form,

$$\begin{aligned}
|v_0\rangle &= \left(1, 0, \sqrt{\cos \pi/5}\right)^T, \\
|v_1\rangle &= \left(\cos 4\pi/5, -\sin 4\pi/5, \sqrt{\cos \pi/5}\right)^T, \\
|v_2\rangle &= \left(\cos 2\pi/5, \sin 2\pi/5, \sqrt{\cos \pi/5}\right)^T, \\
|v_3\rangle &= \left(\cos 2\pi/5, -\sin 2\pi/5, \sqrt{\cos \pi/5}\right)^T, \\
|v_4\rangle &= \left(\cos 4\pi/5, \sin 4\pi/5, \sqrt{\cos \pi/5}\right)^T.
\end{aligned} \tag{6.9}$$

We then optimize $|\phi\rangle$ for maximum value of $\mathcal{K}$ with the exclusivity conditions (6.2) imposed on ζ_i as,

$$\zeta_i + \zeta_{i\oplus 1} \leq 1 \; \forall i \in \{0, 1, 2, 3, 4\}. \tag{6.10}$$

The set of post-selected states in the aforementioned optimization giving rise to probability distributions that do not satisfy Eq. (6.10) is discarded. We then evaluate $\mathcal{K}$ using the rule (6.6) for the measurement $\{\Pi_i, \mathbb{1} - \Pi_i\}$ to assign $P(\Pi_i = 1) = \zeta_i$ accordingly. A schematic diagram for the same is given in Fig. 6.1

It is found that when no exclusivity conditions are imposed on ζ_i, $\max(\mathcal{K}) > 2.25$ which falsely indicates a highly contextual behavior while it is known that quantum theory shows a KCBS violation no greater than 2.25. However, upon proper conditioning we found that no post-selection can lead to a violation of the KCBS inequality. In Fig 6.2 we plot the intersection of the inequalities (6.2) and (6.3) for various minimum values of $\mathcal{K}$ over the entire region of post-selected states. Incidentally we do not find any set of states for which KCBS inequality is violated. This provides a clear evidence of the fact that the ABL formalism does not provide a complete description under the pre- and post-selection paradigm.

It is also interesting to note that when post-selection is removed, we recover back the quantum statistics and are once again able to violate the KCBS inequality to its quantum maximum (6.4). We achieve this by noting that the post-selection is a projective measurement, $\mathcal{M}_{post} := \{|\phi\rangle\langle\phi|, \mathbb{1} - |\phi\rangle\langle\phi|\}$ in which only the outcome $|\phi\rangle\langle\phi|$ is considered. In order to remove the effects of post-selection, it is necessary to consider all the outcomes of $\mathcal{M}_{post}$. Therefore, the final state ρ_f after removal of post-selection is,

$$\rho_f = p_i |\phi\rangle\langle\phi| + (1 - p_i)\left(\mathbb{1} - |\phi\rangle\langle\phi|\right), \tag{6.11}$$

where p_i is the conditional probability of obtaining outcome $|\phi\rangle\langle\phi|$ given the state $|\psi\rangle$ and is given as

$$p_i = |\langle\psi|\phi\rangle|^2. \tag{6.12}$$

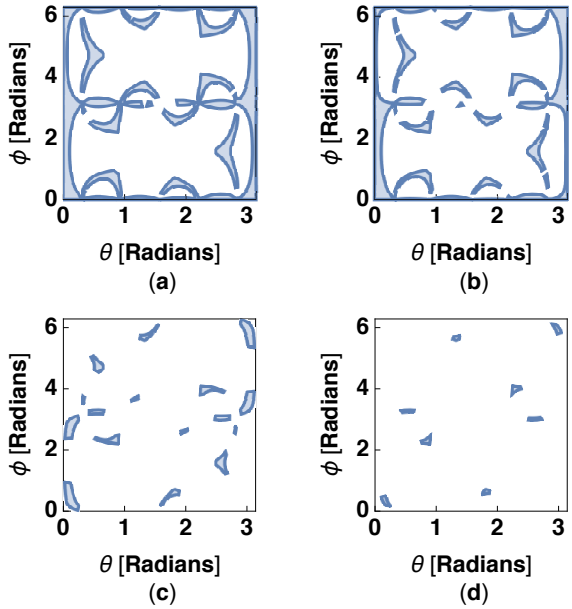

Figure 6.2: A region plot corresponding to a set of post-selected states (6.8) (shaded blue) for which Eqn. (6.2) is satisfied $\forall i$ with (a) $\mathcal{K} > 1.4$, (b) $\mathcal{K} > 1.5$, (c) $\mathcal{K} > 1.6$ and (d) $\mathcal{K} > 1.7$. No set of states were found for $\mathcal{K} > 2.0$.

This final state is formed by a convex mixture of two post-selected states, corresponding to $|\phi\rangle\langle\phi|$ and $\mathbb{1} - |\phi\rangle\langle\phi|$ and physically implies that all possible outcomes to $\mathcal{M}_{post}$ are now considered to analyse the violation of the KCBS scenario. It is to be noted that the removal of post-selection via the aforementioned method does not reduce the ABL rule to the Born rule. The Born rule only depends on the pre-selected state $|\psi\rangle$ and the outcomes of the observable A, while the removal of post-selection in the ABL depends on the convex mixture of all possible post-selected states as well as pre-selected state and the outcomes of A. As is evident, the probability assigned to a particular outcome of A from the Born rule is not the same as assigned from the ABL rule with post-selection removed.

The final state ρ_f obtained after eliminating the effects of post-selection also depends on the parameters θ and ϕ. An optimization over these parameters for maximum value of $\mathcal{K}$ under the constraints of exclusivity conditions yields solution up to $\mathcal{K} < 2.25$, which corresponds to the quantum maximum. The set of all states satisfying the exclusivity condition (6.10) over the parameter space θ and ϕ is shown in Fig. 6.3.

As shown in Fig. 6.2, the ABL rule cannot reproduce contextual correlations, specifically in the well studied KCBS and n-cycle contextuality scenario. We again emphasize that only counterfactual assignments of probabilities from the ABL rule are considered. In Fig. 6.3 we show that it is possible to have a contextual advan-

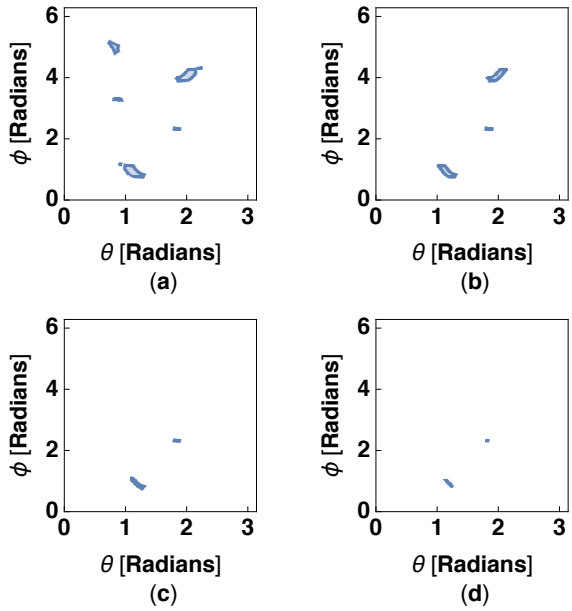

Figure 6.3: A region plot corresponding to a set of final states ρ_f (shaded blue) for which Eqn. (6.2 is satisfied $\forall i$ with (a) $\mathcal{K} > 2.0$, (b) $\mathcal{K} > 2.1$, (c) $\mathcal{K} > 2.2$ and (d) $\mathcal{K} > 2.24$. The violation of the KCBS inequality under elimination of post-selection indicates that the same leads to an incomplete description.

tage once post-selection is removed, which is exactly the quantum scenario. A single proof of failure is sufficient to show that the counterfactual ABL rule is in general non-contextual and cannot capture the complete description of observables in the pre- and post-selection paradigm.

6.4 Conclusion

In this chapter we have focused on PPS scenarios especially in the case of KCBS inequality. We show that the ABL rule to evaluate probability distribution over the outcomes of an observable A in a PPS scenario does not provide a contextual violation of the KCBS inequality. The ABL rule is applied in a counterfactual manner in which the observable A is not necessarily measured. In this case, the ABL rule forms an ontic model of the KCBS inequality with context dependency in the form of pre and post selected states. Upon proper conditioning of the ABL probabilities in the form of exclusivity conditions we found that it is not able to reproduce the statistics that are observed in nature. Essentially, it is found not to violate the KCBS inequality for any set of pre- and post-selected states.

However, once the post-selection is removed, the ABL rule is able to correctly assign the probabilities, such that the KCBS inequality is violated. This hints to a paradoxical nature of post-selection in such scenarios and requires further investigation.

Our results show that the ABL rule is essentially non-contextual contrary to recent studies [11, 112, 113]. Most of the recent studies deal with probability assignments which are not properly conditioned and lead to scenarios where the sum of probabilities of exclusive events can be greater than 1 leading to false signatures of contextuality. We term such scenarios as paradoxical. Furthermore, all of the aforementioned paradoxical scenarios show a contextual behaviour via a logical proof of the same. Such proofs are hard to verify in an experiment. On the other hand we provide a statistical proof which can be readily verified. Furthermore, it is not clear how weak values can be interpreted in terms of probabilities and expectation values as they can take on arbitrary complex numbers.

On the other hand, our results are properly conditioned and explicitly show that ABL rule is non-contextual.

Chapter 7

Summary and future outlook

In this thesis we have analysed novel signatures of quantum contextuality and explored applications of its standard and entropic approaches as well as Bell non-locality in QKD.

In the first project of this thesis we develop a new generalization of the assumption of measurement non-contextuality, which encompasses a much broader range of scenarios than the traditional one developed by Spekkens. As a consequence of this generalization, we find that it is possible to assign a notion of measurement non-contextuality to a single measurement device which is applied sequentially. This drastically reduces the number of measurements required to reveal quantum contextuality, which earlier was 5 for PVMs and 3 for POVMs. Our result opens up several new and interesting scenarios not previously studied and has potential applications in QKD, parity oblivious multiplexing, quantum computation and in various foundational aspects. It is expected that our generalization could lead to robust experimental tests of contextuality as well as state independent proofs of the same, without the assumption of outcome determinism.

In the second project we devise a prepare and measure QKD protocol whose security is based on the monogamy of contextual correlations. We use the KCBS scenario to share a secure key between Alice and Bob and derive the monogamy relationship amongst the three parties including Eve, using a graph theoretic approach. We find that Alice and Bob can share a secure key if they are able to violate the KCBS inequality. Our work shows that state dependent quantum contextuality in terms of n-cycle inequalities can be used to share a secure key. Our work also hints that monogamy of contextuality is an important resource in information processing tasks and requires further investigation. An important aspect of our work is that it does not utilize the costly resource of entanglement and yet provides security via a violation of a fundamental inequality. This feature is almost absent in all prepare and measure schemes,

while being prevalent in entanglement based ones such as E91 and CHSH.

In the third project we apply the idea of monogamy of contextuality to entropic inequalities. In this case we first demonstrate that a graph theoretic approach can be used to derive these relations quite easily for entropic contextual inequalities. We explicitly show when such relationships exist and how they can be derived. We then proceed to apply these relationships to derive security conditions for protocols based on entropic inequalities. We particularly focus on the entropic version of the CHSH inequality which forms a $n = 4$ cycle graph, while our results can be easily generalized for all even n cycles. Entropic inequalities subsume both Bell non-local as well as contextual scenarios, and therefore our results demonstrate how any of these principles can be used to show security of the QKD protocol. Furthermore, entropic inequalities are independent of the number of outcomes, thereby indicating that our results can be easily generalized for all types of measurements with Alice and Bob. Our work acts as a proof of principle that these entropic inequalities can be used for secure QKD, while opening up several new research avenues for their application in other information processing tasks.

For the fourth project we focus on the role of Bell-CHSH violation in entanglement based QKD protocols. It is well known that Bell non-locality is a necessary resource for sharing a secure key, while it is still debatable whether it is sufficient as well. We show that while being a necessary resource it is not sufficient for secure key distribution. We construct a geometrical representation of all two qubit states parametrised by their Bell-CHSH violation and QBER. This representation is expected to be advantageous for experimentalists to check which states are optimal for performing QKD given the two aforementioned parameters in their experiment. From this geometrical representation we show that there exists states that are not useful for QKD even though they exhibit a violation of the Bell-CHSH inequality. We further show that local filtering operations can be used to enhance the secure key rate offered by some states, while transforming some of the useless states for QKD into useful ones. However, not all useless states can be made useful, most notable being the Bell diagonal states. This is true even if they violate the Bell-CHSH inequality. Our work is expected to have a significant impact for experimentalists looking to perform QKD with two qubits.

In the last project we analyse the consequences of applying pre- and post-selection scenarios as ontic models to describe the contextual behaviour of quantum theory. We specifically apply the ABL rule in a counterfactual manner to the operational version of the KCBS inequality and show that it cannot lead to contextual correlations. We further show that uplifting post-selection leads to a contextual description indicating that it might be the root cause of all the paradoxes that have plagued PPS scenarios and weak values. Our work clearly refutes the ABL formalism by providng a simple counter-example and is expected to open up several discussions.

In general, the thesis explores the role of foundational aspects of quantum theory in QKD which can be applied to other communication tasks. In particular, application of contextuality in device independent scenarios seems a promising avenue while local filtering operations in the context of entropic inequalities is still an unexplored territory. Moreover, the connection between non-contextual advantage in PPS scenarios with post-selection needs to be brought into more focus.

References

[1] S. Kochen and E. P. Specker, The Problem of Hidden Variables in Quantum Mechanics, Journal of Mathematics and Mechanics **17**, 59–87 (1967). 2, 17, 27, 39, 73

[2] A. Peres, Two simple proofs of the Kochen-Specker theorem, Journal of Physics A Mathematical General **24** (Feb. 1991). 2

[3] A. Peres, *Quantum Theory: Concepts and Methods*, Fundamental Theories of Physics, Springer, 1995. 2, 3

[4] A. Cabello, M. Kleinmann, and C. Budroni, Necessary and Sufficient Condition for Quantum State-Independent Contextuality, Phys. Rev. Lett. **114**, 250402 (Jun 2015). 2, 6, 17

[5] S. Yu and C. H. Oh, State-Independent Proof of Kochen-Specker Theorem with 13 Rays, Phys. Rev. Lett. **108**, 030402 (Jan 2012). 2, 6, 17

[6] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky, Simple Test for Hidden Variables in Spin-1 Systems, Phys. Rev. Lett. **101**, 020403 (Jul 2008). 2, 4, 5, 17, 27, 28, 39, 74

[7] R. W. Spekkens, Contextuality for preparations, transformations, and unsharp measurements, Phys. Rev. A **71**, 052108 (May 2005). 2, 17, 18, 76

[8] S. L. Braunstein and C. M. Caves, Information-Theoretic Bell Inequalities, Phys. Rev. Lett. **61**, 662–665 (Aug 1988). 2, 40

[9] R. Chaves, Entropic inequalities as a necessary and sufficient condition to non-contextuality and locality, Phys. Rev. A **87**, 022102 (Feb 2013). 2, 40

[10] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880–884 (Oct 1969). 2, 9, 17, 39, 55

[11] M. S. Leifer and R. W. Spekkens, Pre- and Post-Selection Paradoxes and Contextuality in Quantum Mechanics, Phys. Rev. Lett. **95**, 200405 (Nov 2005). 3, 74, 81

[12] A. Acín, T. Fritz, A. Leverrier, and A. B. Sainz, A Combinatorial Approach to Nonlocality and Contextuality, Communications in Mathematical Physics **334**(2), 533–628 (2015). 5, 7, 17, 39

[13] B. Amaral, M. T. Cunha, and A. Cabello, Exclusivity principle forbids sets of correlations larger than the quantum set, Phys. Rev. A **89**, 030101 (Mar 2014). 5, 17, 39

[14] Y.-C. Liang, R. W. Spekkens, and H. M. Wiseman, Specker's parable of the overprotective seer: A road to contextuality, nonlocality and complementarity, Physics Reports **506**(1-2), 1 – 39 (2011). 6, 17

[15] S. Dogra, K. Dorai, and Arvind, Experimental demonstration of quantum contextuality on an NMR qutrit, Physics Letters A **380**(22), 1941 – 1946 (2016). 6, 39

[16] D. Singh, J. Singh, K. Dorai, and Arvind, Experimental demonstration of fully contextual quantum correlations on an NMR quantum information processor, Phys. Rev. A **100**, 022109 (Aug 2019). 6

[17] T. Li, Q. Zeng, X. Song, and X. Zhang, Experimental contextuality in classical light, Scientific Reports **7**(1), 44467 (2017). 6

[18] A. Cabello, Experimentally Testable State-Independent Quantum Contextuality, Phys. Rev. Lett. **101**, 210401 (Nov 2008). 6

[19] W. Tang and S. Yu, Construction of state-independent proofs for quantum contextuality, Phys. Rev. A **96**, 062126 (Dec 2017). 6

[20] A. Cabello, S. Severini, and A. Winter, Graph-Theoretic Approach to Quantum Correlations, Phys. Rev. Lett. **112**, 040401 (Jan 2014). 6, 17, 28, 39

[21] R. Ramanathan, A. Soeda, P. Kurzyński, and D. Kaszlikowski, Generalized Monogamy of Contextual Inequalities from the No-Disturbance Principle, Phys. Rev. Lett. **109**, 050404 (Aug 2012). 8, 17, 28, 29, 34, 38, 46

[22] P. Kurzyński, A. Cabello, and D. Kaszlikowski, Fundamental Monogamy Relation between Contextuality and Nonlocality, Phys. Rev. Lett. **112**, 100401 (Mar 2014). 8, 17

[23] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, Phys. Rev. **47**, 777–780 (May 1935). 9, 27, 55

[24] J. S. Bell, On the einstein-podolsky-rosen paradox, Physics **1**(3), 195–200 (1964). 9, 27

[25] J. S. BELL, On the Problem of Hidden Variables in Quantum Mechanics, Rev. Mod. Phys. **38**, 447–452 (Jul 1966). 9, 17, 39

[26] N. D. Mermin, Hidden variables and the two theorems of John Bell, Rev. Mod. Phys. **65**, 803–815 (Jul 1993). 9, 73

[27] N. D. Mermin, Is the Moon There When Nobody Looks? Reality and the Quantum Theory, Physics Today **38**(4), 38–47 (1985). 9

[28] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, BellâĂŹs theorem without inequalities, American Journal of Physics **58**(12), 1131–1143 (1990). 9

[29] A. Fine, Hidden Variables, Joint Probability, and the Bell Inequalities, Phys. Rev. Lett. **48**, 291–295 (Feb 1982). 9

[30] A. Fine, Joint distributions, quantum correlations, and commuting observables, Journal of Mathematical Physics **23**(7), 1306–1310 (1982). 9

[31] D. Bohm, A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I, Phys. Rev. **85**, 166–179 (Jan 1952). 9

[32] M. M. Wilde, *Quantum Information Theory*, Cambridge University Press, 2013. 10

[33] R. Sridhar and R. Simon, Normal form for Mueller Matrices in Polarization Optics, Journal of Modern Optics **41**(10), 1903–1915 (1994). 10, 60

[34] B. S. Cirel'son, Quantum generalizations of Bell's inequality, Letters in Mathematical Physics **4**(2), 93–100 (1980). 10, 11

[35] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419–478 (Apr 2014). 17, 39, 55

[36] M. Araújo, M. T. Quintino, C. Budroni, M. T. Cunha, and A. Cabello, All noncontextuality inequalities for the n-cycle scenario, Phys. Rev. A **88**, 022118 (Aug 2013). 17, 39

[37] P. Kurzyński and D. Kaszlikowski, Contextuality of almost all qutrit states can be revealed with nine observables, Phys. Rev. A **86**, 042125 (Oct 2012). 17

[38] P. Lisoněk, P. Badziąg, J. R. Portillo, and A. Cabello, Kochen-Specker set with seven contexts, Phys. Rev. A **89**, 042101 (Apr 2014). 17

[39] M. Kleinmann, C. Budroni, J.-A. Larsson, O. Gühne, and A. Cabello, Optimal Inequalities for State-Independent Contextuality, Phys. Rev. Lett. **109**, 250402 (Dec 2012). 17

[40] A. Cabello, M. Kleinmann, and J. R. Portillo, Quantum state-independent contextuality requires 13 rays, Journal of Physics A: Mathematical and Theoretical **49**(38), 38LT01 (aug 2016). 17

[41] A. Cabello, Twin inequality for fully contextual quantum correlations, Phys. Rev. A **87**, 010104 (Jan 2013). 17

[42] K. Bharti, M. Ray, and L.-C. Kwek, Non-Classical Correlations in n-Cycle Setting, Entropy **21**(2) (2019). 17

[43] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L.-C. Kwek, Robust self-testing of quantum systems via noncontextuality inequalities, (Dec 2018). 17

[44] J. Singh, K. Bharti, and Arvind, Quantum key distribution protocol based on contextuality monogamy, Phys. Rev. A **95**, 062333 (Jun 2017). 17, 39, 55

[45] A. Cabello, V. D'Ambrosio, E. Nagali, and F. Sciarrino, Hybrid ququart-encoded quantum cryptography protected by Kochen-Specker contextuality, Phys. Rev. A **84**, 030302 (Sep 2011). 17, 28

[46] J. E. Troupe and J. M. Farinholt, A Contextuality Based Quantum Key Distribution Protocol, (Dec 2015). 17

[47] R. Kunjwal and S. Ghosh, Minimal state-dependent proof of measurement contextuality for a qubit, Phys. Rev. A **89**, 042118 (Apr 2014). 17, 18

[48] R. Kunjwal and R. W. Spekkens, From the Kochen-Specker Theorem to Noncontextuality Inequalities without Assuming Determinism, Phys. Rev. Lett. **115**, 110403 (Sep 2015). 17, 20

[49] R. Kunjwal and R. W. Spekkens, From statistical proofs of the Kochen-Specker theorem to noise-robust noncontextuality inequalities, Phys. Rev. A **97**, 052110 (May 2018). 17, 20

[50] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Preparation Contextuality Powers Parity-Oblivious Multiplexing, Phys. Rev. Lett. **102**, 010401 (Jan 2009). 18

[51] A. Chailloux, I. Kerenidis, S. Kundu, and J. Sikora, Optimal bounds for parity-oblivious random access codes, New Journal of Physics **18**(4), 045003 (apr 2016). 18

[52] A. Ambainis, M. Banik, A. Chaturvedi, D. Kravchenko, and A. Rai, Parity oblivious d-level random access codes and class of noncontextuality inequalities, Quantum Information Processing **18**(4), 111 (Mar 2019). 18

[53] M. D. Mazurek, M. F. Pusey, R. Kunjwal, K. J. Resch, and R. W. Spekkens, An experimental test of noncontextuality without unphysical idealizations, Nature Communications **7**(1), ncomms11780 (2016). 20

[54] M. Pawłowski and C. Brukner, Monogamy of Bell's Inequality Violations in Nonsignaling Theories, Phys. Rev. Lett. **102**, 030403 (Jan 2009). 28

[55] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, New York, NY, USA, 10th edition, 2011. 28

[56] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145–195 (Mar 2002). 28, 55

[57] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301–1350 (Sep 2009). 28, 55

[58] A. Acín, N. Gisin, and L. Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. **97**, 120405 (Sep 2006). 28, 39, 40, 53, 54, 55, 56, 64

[59] M. Pawłowski, Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations, Phys. Rev. A **82**, 032313 (Sep 2010). 28, 35, 39, 40, 53, 54, 55

[60] C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, 1984, IEEE Press. 28, 55

[61] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661–663 (Aug 1991). 28

[62] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121–3124 (May 1992). 28

[63] H. Bechmann-Pasquinucci and A. Peres, Quantum Cryptography with 3-State Systems, Phys. Rev. Lett. **85**, 3313–3316 (Oct 2000). 28, 32

[64] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441–444 (Jul 2000). 28, 55

[65] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Security of two quantum cryptography protocols using the same four qubit states, Phys. Rev. A **72**, 032301 (Sep 2005). 28, 55

[66] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, Performance of two quantum-key-distribution protocols, Phys. Rev. A **73**, 012337 (Jan 2006). 28, 55

[67] I. Csiszar and J. Korner, Broadcast channels with confidential messages, IEEE Transactions on Information Theory **24**(3), 339–348 (May 1978). 36

[68] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Bell Inequalities for Arbitrarily High-Dimensional Systems, Phys. Rev. Lett. **88**, 040404 (Jan 2002). 39, 55

[69] J.-A. Larsson, M. Giustina, J. Kofler, B. Wittmann, R. Ursin, and S. Ramelow, Bell-inequality violation with entangled photons, free of the coincidence-time loophole, Phys. Rev. A **90**, 032107 (Sep 2014). 39

[70] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (Dec 2015). 39

[71] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Strong Loophole-Free Test of Local Realism, Phys. Rev. Lett. **115**, 250402 (Dec 2015). 39

[72] G. Kirchmair, F. Zähringer, R. Gerritsma, M. Kleinmann, O. Gühne, A. Cabello, R. Blatt, and C. F. Roos, State-independent experimental test of quantum contextuality, Nature **460**, 494 EP – (07 2009). 39

[73] S. Popescu and D. Rohrlich, Which states violate Bell's inequality maximally?, Physics Letters A **169**(6), 411 – 414 (1992). 39

[74] S. L. Braunstein, A. Mann, and M. Revzen, Maximal violation of Bell inequalities for mixed states, Phys. Rev. Lett. **68**, 3259–3261 (Jun 1992). 39

[75] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, Npj Quantum Information **2**, 16025 EP – (11 2016). 39

[76] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (Sep 2014). 39

[77] A. Acín and L. Masanes, Certified randomness in quantum physics, Nature **540**, 213 EP – (12 2016). 39

[78] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (Jun 2007). 39

[79] R. Chaves and C. Budroni, Entropic Nonsignaling Correlations, Phys. Rev. Lett. **116**, 240501 (Jun 2016). 40, 42, 50

[80] R. Chaves and T. Fritz, Entropic approach to local realism and noncontextuality, Phys. Rev. A **85**, 032113 (Mar 2012). 40

[81] L.-Z. Cao, J.-Q. Zhao, X. Liu, Y. Yang, Y.-D. Li, X.-Q. Wang, Z.-B. Chen, and H.-X. Lu, Experimental investigation of the information entropic Bell inequality, Scientific Reports **6**, 23758 EP – (04 2016). 40

[82] S. Popescu and D. Rohrlich, Quantum nonlocality as an axiom, Foundations of Physics **24**(3), 379–385 (1994). 42

[83] C. Kumar, J. Singh, S. Bose, and Arvind, Coherence-assisted non-Gaussian measurement-device-independent quantum key distribution, Phys. Rev. A **100**, 052329 (Nov 2019). 55

[84] R. Augusiak, D. Cavalcanti, G. Prettico, and A. Acín, Perfect Quantum Privacy Implies Nonlocality, Phys. Rev. Lett. **104**, 230401 (Jun 2010). 55

[85] Č. Brukner and M. Żukowski, *Bell's Inequalities — Foundations and Quantum Communication*, pages 1413–1450, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012. 55

[86] A. Ferenczi and N. Lütkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, Phys. Rev. A **85**, 052310 (May 2012). 55, 58, 59, 62, 64

[87] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277–4281 (Oct 1989). 55

[88] M. Froissart, Constructive generalization of Bell's inequalities, 1981. 55

[89] D. Collins and N. Gisin, A relevant two qubit Bell inequality inequivalent to the CHSH inequality, Journal of Physics A: Mathematical and General **37**(5), 1775 (2004). 55, 56

[90] A. Acín, L. Masanes, and N. Gisin, Equivalence between Two-Qubit Entanglement and Secure Key Distribution, Phys. Rev. Lett. **91**, 167901 (Oct 2003). 56

[91] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Secure Key from Bound Entanglement, Phys. Rev. Lett. **94**, 160502 (Apr 2005). 56

[92] F. Verstraete, J. Dehaene, and B. DeMoor, Local filtering operations on two qubits, Phys. Rev. A **64**, 010101 (Jun 2001). 56, 60, 69, 71

[93] Z.-W. Wang, X.-F. Zhou, Y.-F. Huang, Y.-S. Zhang, X.-F. Ren, and G.-C. Guo, Experimental Entanglement Distillation of Two-Qubit Mixed States under Local Operations, Phys. Rev. Lett. **96**, 220505 (Jun 2006). 57

[94] W. K. Wootters, Entanglement of Formation of an Arbitrary State of Two Qubits, Phys. Rev. Lett. **80**, 2245–2248 (Mar 1998). 59, 61

[95] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865–942 (Jun 2009). 59, 61

[96] N. Gisin, Hidden quantum nonlocality revealed by local filters, Physics Letters A **210**(3), 151–156 (jan 1996). 59, 69

[97] R. Pal and S. Ghosh, A closed-form necessary and sufficient condition for any two-qubit state to show hidden nonlocality w.r.t the Bell-CHSH inequality. 60

[98] D. Pastorello, A quantum key distribution scheme based on tripartite entanglement and violation of CHSH inequality, International Journal of Quantum Information **15**(05), 1750040 (2017). 64

[99] Y. Aharonov, P. G. Bergmann, and J. L. Lebowitz, Time Symmetry in the Quantum Process of Measurement, Phys. Rev. **134**, B1410–B1416 (Jun 1964). 73

[100] Y. Aharonov, D. Z. Albert, and L. Vaidman, How the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100, Phys. Rev. Lett. **60**, 1351–1354 (Apr 1988). 73

[101] Y. Aharonov and L. Vaidman, Complete description of a quantum system at a given time, Journal of Physics A: Mathematical and General **24**(10), 2315 (1991). 73

[102] L. Vaidman, Tracing the past of a quantum particle, Phys. Rev. A **89**, 024102 (Feb 2014). 73

[103] Y. Aharonov, A. Botero, S. Popescu, B. Reznik, and J. Tollaksen, Revisiting Hardy's paradox: counterfactual statements, real measurements, entanglement and weak values, Physics Letters A **301**(3), 130 – 138 (2002). 73

[104] T. Denkmayr, H. Geppert, S. Sponar, H. Lemmel, A. Matzkin, J. Tollaksen, and Y. Hasegawa, Observation of a quantum Cheshire Cat in a matter-wave interferometer experiment, Nature Communications **5**, 4492 EP – (Jul 2014), Article. 73

[105] A. Danan, D. Farfurnik, S. Bar-Ad, and L. Vaidman, Asking Photons Where They Have Been, Phys. Rev. Lett. **111**, 240402 (Dec 2013). 73

[106] J. S. Lundeen and A. M. Steinberg, Experimental Joint Weak Measurement on a Photon Pair as a Probe of Hardy's Paradox, Phys. Rev. Lett. **102**, 020404 (Jan 2009). 73

[107] K. Resch, J. Lundeen, and A. Steinberg, Experimental realization of the quantum box problem, Physics Letters A **324**(2), 125 – 131 (2004). 73

[108] Z.-H. Liu, W.-W. Pan, X.-Y. Xu, M. Yang, J. Zhou, Z.-Y. Luo, K. Sun, J.-L. Chen, J.-S. Xu, C.-F. Li, and G.-C. Guo, Experimental exchange of grins between quantum Cheshire cats, Nature Communications **11**(1), 3006 (Jun 2020). 73

[109] D. Z. Albert, Y. Aharonov, and S. D'Amato, Curious New Statistical Prediction of Quantum Mechanics, Phys. Rev. Lett. **54**, 5–7 (Jan 1985). 73

[110] J. Bub and H. Brown, Curious Properties of Quantum Ensembles Which Have Been Both Preselected and Post-Selected, Phys. Rev. Lett. **56**, 2337–2340 (Jun 1986). 73

[111] N. D. Mermin, Limits to Quantum Mechanics as a Source of Magic Tricks: Retrodiction and the Bell-Kochen-Specker Theorem, Phys. Rev. Lett. **74**, 831–834 (Feb 1995). 74

[112] M. F. Pusey, Anomalous Weak Values Are Proofs of Contextuality, Phys. Rev. Lett. **113**, 200401 (Nov 2014). 74, 81

[113] R. Kunjwal, M. Lostaglio, and M. F. Pusey, Anomalous weak values and contextuality: Robustness, tightness, and imaginary parts, Phys. Rev. A **100**, 042116 (Oct 2019). 74, 81