Quantum Correlations and Its Applications

Kishor Bharti

A dissertation submitted for the partial fulfilment
of BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali
April 2016

Certificate of Examination

This is to certify that the dissertation titled **Quantum Correlations and Its Applications** submitted by **Kishor Bharti** (Reg. No. MS11016) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Kavita Dorai Dr. K. P. Singh Prof. Arvind
(Supervisor)

Dated: April 22, 2016

Declaration

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

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is 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.

Kishor Bharti
(Candidate)

Dated: April 22, 2016

In my capacity as the supervisor of the candidates project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Prof. Arvind
(Supervisor)

Acknowledgment

The master thesis was guided by Prof. Arvind and I thank him for his both academic as well as non-academic support throughout the course of the project. He provided me the optimum independence to pursue my interest. Moreover, I thank him for providing the office space, organizing group seminars and discussion sessions.

I would like to thank Atul, Bhati and Jaskaran for various fruitful discussions. These discussions were conducive in understanding and applying quantum information for the master thesis. In particular, discussions with Jaskaran helped me understand contextuality better. I would like to thank other QCQI group members, in particular Varinder Singh and Debmalya Das for their support during the course of the support.

I would further like to thank Atul, Prashansa, Manvendra Rajvanshi, Gyanendra, Hemanshu, Shubham, Vivek Singh, Bhati, Jaskaran, Nakul and many other friends from IISER (whom I would like to thank, but due to limited space can't do so on individual basis) for their effort in making my life at IISER pleasant during the course of project.

At last, I would like to thank IISER Mohali Community, KVPY and MHRD for providing the logistic support.

List of Figures

Notation

$\mathbb{I}$	Identity Matrix (in appropriate dimensions)
$\mathbb{C}^n$	Hilbert space, dimension n
ρ	Density matrix
$\mathcal{W}$	Entanglement witness
$\mathcal{H}_A$	Hilbert space of Alice
$\mathcal{H}_B$	Hilbert space of Bob

Contents

Abstract

In this work, we try to understand and characterize quantum correlations. Attempts have been made to focus on the key ingredients of quantum mechanics which differentiate quantum correlations from the classical ones. The thesis focuses on entanglement, its manifestation as Bell nonlocality, quantum contextuality and discord. Furthermore, we try to analyze the implications of quantum correlations for device independent quantum key distribution and to understand the foundations of quantum mechanics at a deeper level.

Chapter 1

Background

1.1 Correlations

Correlations among multiple parties is witnessed both in classical as well as in quantum regime. Violation of Bell inequalities is one such example in quantum world. The way stock markets behave after a cricket match or an election result show some correlations as well and can be studied to understand classical correlations. [Sca13]

Formally speaking, *two or more parties are correlated if together they contain more information than taken separately* [MBC+12]. Hence, mutual information seems the right tool to quantify the amount of correlations among multiple parties. The lack of information is given by entropy, consequently mutual information between parties A and B turns out to be

$$I(A:B) = S(A) + S(B) - S(AB) \tag{1.1}$$

where

- $S(X)$ is Shannon entropy given by $S(X) = -\Sigma_x p_x \log p_x$ if X is a classical variable with values x occurring with probability p_x
- $S(X)$ is Von Neumann entropy given by $S(X) = -tr(\rho_x \log \rho_x)$ where ρ_x represents the quantum state of system X

1.1.1 Quantum vs Classical correlations

For classical variables, we know that

$$P_{x|y} = \frac{P_{xy}}{P_y}. \tag{1.2}$$

It leads to an equivalent form for the classical mutual information:

$$J_{\mathsf{cl}}(B|A) = S(B) - S(B|A), \tag{1.3}$$

where

$$S(B|A) = \Sigma_a P_a S(B|a) \tag{1.4}$$

and

$$S(B|a) = -\Sigma_b P_{b|a} \log P_{b|a}. \tag{1.5}$$

Thus, one can interpret classical correlations as information gain about one subsystem due to a measurement on the another.

The quantum analog, on the other hand, does not fit into this classical definition due to following reasons [MBC+12]:

- There are many different measurements that can be performed on a system
- Measurements disturb the system under consideration (quantum state)

Furthermore, quantum correlations can be modeled in terms of quantum resources. To understand quantum correlations, we need to understand Entanglement, Quantum Discord and Quantum Contextuality.

1.2 Entanglement

Let $\mathcal{H}$ be the combined Hilbert space of an Alice-Bob system (A and B), given as

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B. \tag{1.6}$$

A pure state $|\psi\rangle \in \mathcal{H}$ shared by two parties Alice and Bob is called separable if and only if it can be written as [NC11]

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \tag{1.7}$$

In density operator formalism, a mixed bipartite state (between Alice and Bob) ρ is called separable if and only if it can be written as a convex sum of pure product states [NC11] i.e

$$\rho = \Sigma_i P_i |\psi_i^A\rangle\langle\psi_i^A| \otimes |\psi_i^B\rangle\langle\psi_i^B| \tag{1.8}$$

$$P_i \geq 0 \tag{1.9}$$

$$\Sigma_i P_i = 1. \tag{1.10}$$

Otherwise the state is **entangled**.

1.2.1 Witnessing Entanglement

Hahn Banach theorem guarantees that given [Cla06]

- a convex set, and
- a point lying outside the set,

these two can be separated by a hyper-plane $\mathcal{W}$. Riesz-Frechet representation characterizes such hyperplanes $\mathcal{W}$. Here, $\mathcal{W}$ is called witness. In the Hilbert space formalism, let

$$\mathcal{C} \subset \mathcal{D} \tag{1.11}$$

where $\mathcal{D}$ is the set of normalized positive semidefinite operators (constituted by density operators ρ) and $\mathcal{C}$ is the convex subset of states in Hilbert space $\mathcal{H}$. Then for $\rho \notin \mathcal{C}$, $\exists$ A such that

$$Tr(A\rho) < 0 \tag{1.12}$$

and

$$Tr(A\sigma) \geq 0, \tag{1.13}$$

$\forall\, \sigma \in \mathcal{C}$. This motivates us to develop the following criteria for separability.

Separability criteria

Given $\rho \in \mathcal{D}$, it is separable iff [Cla06]

$$Tr(\rho\mathcal{W}) \geq 0, \tag{1.14}$$

$\forall$ Hermitian operators $\mathcal{W}$ such that

$$Tr([|\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B|]\mathcal{W}) \geq 0, \tag{1.15}$$

where subscripts (A/B) denotes the respective Hilbert spaces. $\mathcal{W}$ is referred as entanglement witness.

Examples

Here are a few entanglement witnesses.

- For a given operator F such that $F|\psi_A\rangle\langle\psi_B| = |\psi_B\rangle\langle\psi_A|$. F can be explicitly written as $F = \Sigma_{i,j}|ij\rangle\langle ji|$. One can verify that F can be used to detect entanglement in $S = |\psi_-\rangle\langle\psi_-|$, where $|\psi_-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$
- One can have $\mathcal{W}_R = \mathbb{I} - dP_+$ as entanglement witness, where P_+ is a projector onto the maximally entangled state and d is the dimension of the space.

1.2.2 LOCC and Entanglement distillation

LOCC stands for local operations and classical communication. For a bipartite scenario (Alice and BOb), it means [NC11]:

- Alice and Bob can perform arbitrary operations on their local systems, including measurement.
- They can communicate using classical communication

One can grasp the LOCC protocols by developing an algorithm to convert convert $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ to $|\phi\rangle = cos(\theta)|00\rangle + sin(\theta)|11\rangle$.

1.2.3 Bell Inequalities

To understand Bell inequalities, let us focus on Bell experiments [Sca13].

Bell experiments

In a typical bell experiment:

- Alice and Bob are at distinct locations.
- Each has a measurement device, which should be treated as black box with an input (a knob to select the measurement setting) and an output.

- In every iteration of the experiment, each party sets the knob at a randomly chosen position and receives an outcome.

Let us stick with the following notation:

- Alice's input: x $\in \mathcal{X} = 1, 2, 3, ..., M_A$
- Bob's input: y $\in \mathcal{Y} = 1, 2, 3, ..., M_B$
- Alice's output: a $\in \mathcal{A} = 1, 2, 3, ..., m_A$
- Alice's input: b $\in \mathcal{B} = 1, 2, 3, ..., m_B$

After finitely many iterations of the experiment, Alice and Bob generate $M_A \times M_B$ probability distributions given by

$$\mathcal{P}_{\mathcal{X},\mathcal{Y}} = P(a, b|x, y), a \in \mathcal{A}, b \in \mathcal{B}, x \in \mathcal{X}, y \in \mathcal{Y}. \tag{1.16}$$

Since the experiment runs for finitely many times, we will call these observed statistics. The next task is to explain the observed statistics using *one's favorite explanation*.

Describing the observed statistics

Without loss of generality, we can write

$$P(a, b|x, y) = \int d\lambda \rho(\lambda|x, y) P(a, b|x, y, \lambda), \tag{1.17}$$

$$\rho(\lambda|x, y) \geq 0, \tag{1.18}$$

$$\int d\lambda \rho(\lambda|x, y) = 1. \tag{1.19}$$

Here $P(a, b|x, y, \lambda)$ are valid probability distributions. λ can be called one's favorite explanation. Let us look at a few examples.

- **Quantum theory as the favorite explanation :** Suppose quantum theory is your favorite explanation. You will look for
  - a state ρ

– M_A POVMs $M^x = (E_a^x | a \in \mathcal{A})$

– M_B POVMs $M^y = (E_b^y | b \in \mathcal{B})$

such that

$$\rho(\lambda|x,y) = \delta(\lambda - \rho), \tag{1.20}$$

$$P(a,b|x,y,\lambda) = Tr(\lambda E_a^x \otimes E_b^y). \tag{1.21}$$

You would see that

$$P_Q(a,b|x,y) = \int d\lambda \rho(\lambda - \rho) Tr(\lambda E_a^x \otimes E_b^y) \tag{1.22}$$

$$= Tr(\rho E_a^x \otimes E_b^y) \tag{1.23}$$

which looks familiar!

- **Deterministic explanation :** One can have deterministic explanations also where the outcomes are uniquely determined by inputs.

$$P(a,b|x,y,\lambda) = \delta(a,b) = F(x,y,\lambda), \tag{1.24}$$

$$\delta_{a=f(x,y,\lambda)} \delta_{b=g(x,y.\lambda)}, \tag{1.25}$$

The last equation simply means that if the pair (a,b) is uniquely determined from the input, then a is uniquely determined and b is uniquely determined.

Correlations among distant parties can be classically explained through the following two mechanisms only:

- Communication or signalling
- pre established agreement

let us resort to local explanations/local hidden variables (LV) only.

$$P(a,b|x,y,\lambda) = P(a|x,\lambda)P(b|y,\lambda) \tag{1.26}$$

The fact that $a(b)$ should not depend on $y(x)$ is called **no signalling condition.**

To further understand the Bell Scenario $(\mathcal{X}, \mathcal{A}, \mathcal{Y}, \mathcal{B})$, it is important to mention a couple of theorems from probability theory.

- **Theorem 1** For any fixed scenario, the set $\mathcal{L}$ of probability distributions that can be obtained with LV is convex [Sca13] i.e. if

$$P_1 \in \mathcal{L} \tag{1.27}$$

and

$$P_2 \in \mathcal{L} \tag{1.28}$$

then

$$q.P_1 + (1-q).P_2 \in \mathcal{L} \, \forall q \, \in [0,1] \tag{1.29}$$

- **Theorem 2** A family of probability distributions $\mathcal{P}_{\mathcal{X},\mathcal{Y}} \, \in \mathcal{L}$ can be explained with pre-established with pre established agreement iff it can be explained with deterministic local variables [Sca13].

The local variable statistics can always be explained by a deterministic model. It does not mean that such an explanation must necessarily be adopted. One's favorite explanation as well as the actual explanation can be probabilistic in nature. Now based on the above two theorems one can infer that any $\mathcal{P} \in \mathcal{L}$ can be written as a convex sum of deterministic local variables. Furthermore, every deterministic local point is an extremal point of $\mathcal{L}$ and there are finitely many such points: $m_A^{M_A} m_B^{M_B}$.

A convex set with finitely many extremal points is commonly referred as *Polytope*. This means, $\mathcal{L}$ is the local polytope for the scenario $(\mathcal{X}, \mathcal{A}, \mathcal{Y}, \mathcal{B})$. A polytope $\mathcal{L}$ embedded in $\mathbb{R}^D$ is delimited by $D-1$ dimensional hyperplanes called *facets*. The inequalities associated to the non-trivial facets of $\mathcal{L}$ are the Bell inequalities for the scenario under study.

1.2.4 Bound Entanglement

Suppose we are provided with large number (say n) of maximally entangled states $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, and our goal is to produce with high-fidelity as many copies of some pure state $|\psi\rangle$ using LOCC. If the number of such copies of $|\psi\rangle$ which could be produced is m, the limiting value of $\frac{n}{m}$ is called **entanglement of formation** of $|\psi\rangle$. Similarly, one could look for a process to produce n copies of maximally entangled state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ from m copies of $|\psi\rangle$, the limiting value of $\frac{n}{m}$ is called **distillable entanglement** [NC11] of $|\psi\rangle$.

But as it turns out one can't carry out distillation for all possible entangled $|\psi\rangle$. This motivates us to classify entanglement in two broad categories:

- **Free (or distillable) entanglement:** The entangled state from which one can distill a pure entanglement (useful for quantum communication purposes) by LOCC
- **Bound (or nondistillable) entanglement:** an entangled state which is not distillable.

Thus we can see that the phenomenon of entanglement shows irreversibly. While entanglement is required to prepare a bound entangled state, but entanglement can't be harnessed from a bound entangled state by LOCC. It motivated Peres to think whether bound entangled state can violate a Bell inequality. In 1999 Peres conjectured that *no bound entangled state can give rise to non-local correlations* [Per98].

1.3 Contextuality in a nutshell

Quantum theory is weird in the sense that outcomes of measurements depends upon their context. A context is defined as a set of mutually compatible observables. An observable measured in one context can give a different outcome if measured in a different context. Like Bell's theorem it also allows for correlations among the measurements which are bounded by classical theories. This bound is violated by quantum theory, indicating a non-classical description of reality.

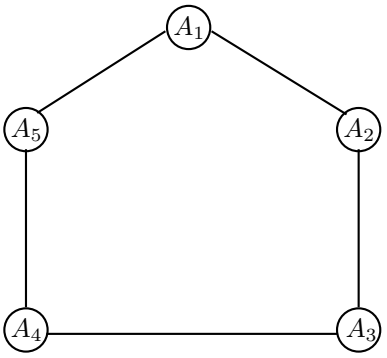

Figure 1.1: KCBS orthogonality graph

Quantum contextuality is more fundamental than Bell's theorem as it does not impose an additional assumption of locality on the system. The first contextuality inequality was given by Kochen and Specker, and it utilized 117 different projectors in a 3 dimensional Hilbert space to arrive at a violation. A more simpler and experimentally realizable inequality is the KCBS inequality, which utilizes only 5 projectors in a 3 dimensional Hilbert space. The inequality states that

$$\sum_{i=1}^{5} P(A_i = 1) \leq 2, \tag{1.30}$$

Where the observables A_i are projectors which cyclically commute. The sum is taken modulo 5. The orthogonality relationship among the observables is best represented by a graph, in which the observables are represented as vertices and commuting observables are joined by a line..

The above inequality is maximally violated by the state $|\gamma\rangle = (0, 0, 1)^T$.

1.4 Discord

Discord is a measure of non-classical correlations between two subsystems of a quantum system. It captures correlations which are quantum mechanical, but may not involve entanglement. For a bipartite system (A and B), a measurement on subsystem A is often described using a positive-operator valued measure with elements given

as $E_a = M_a^\dagger M_a$, where M_a is the measurement operator and a stands for the classical outcome. The state ρ_{AB} is transformed as

$$\rho_{AB} \to \rho'_{AB} = \Sigma_a M_a \rho_{AB} M_a^\dagger. \tag{1.31}$$

Here, Alice(A) gets outcome a with probability $p_a = tr(E_a \rho_{AB})$ and Bob(B) gets the conditional state

$$\rho_{B|a} = \frac{tr_A(E_A \rho_{AB})}{P_a}. \tag{1.32}$$

We can use it to define a classical-quantum analogue of the conditional entropy:

$$S(B|\{E_a\}) \equiv \Sigma_a p_a S(\rho_{B|a}). \tag{1.33}$$

It helps us to introduce classical correlations of the state ρ_{AB} as

$$J(B|\{E_a\}) \equiv S(B) - S(B|\{E_a\}). \tag{1.34}$$

In order to compute the measurement independent classical correlations of the state, $J(B|\{E_a\})$ is maximized over the complete set of measurements,

$$J(B|E_a) \equiv max_{\{E_a\}} J(B|\{E_a\}). \tag{1.35}$$

Now we have gathered all the mathematical tools to precisely define quantum discord. For a state ρ_{AB}, *quantum discord under a measurement* $\{E_a\}$ *is defined as the difference between total correlations and the classical correlations.* [MBC+12]

$$D(B|A) \equiv I(A:B) - J(B|A) \tag{1.36}$$

1.4.1 Properties of discord

- Discord is not symmetric, which means in general $D(B|A) \neq D(A|B)$. This follows from the fact that conditional entropy is not symmetric.

- Discord is non negative. This follows from the concavity of conditional entropy.
- Discord is invariant under local unitary transformations.
- $D(B|A) \geq S(A)$

Chapter 2

Results and Comments

2.1 Hybrid Ekert Protocol

Ekert protocol is an entanglement based quantum key distribution protocol. It utilizes the entanglement of maximally entangled states for secure communication. The key rate of the protocol is 5o percent, which can be improved if we harness the contextual nature of quantum mechanics.

2.1.1 Ekert Protocol

Let us discuss the key ingredients of Ekert protocol [Eke91].

- Alice and Bob want to communicate secretly. We have an eavesdropper, say Eve.
- At the start of every iteration of the protocol, Alice and Bob receive one qubit each from the entangled Bell state ($|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$)
- Alice tosses a coin and gets either Head or Tail.
- If she gets a tail, she measures her qubit in Z basis otherwise in X basis.
- Similarly, Bob tosses a coin as well. If he gets a tail, he measures his qubit in Z basis otherwise in X basis.

- Both publish their coin toss results in public.
- For the cases where they happened to have same coin toss results (which happens half of the times) and consequently measurement in the same basis, they keep the measurement results in the data-set.
- The unmatched cases are discarded.

Clearly, the key rate of the protocol is 50 percent. Part of the key can be used for security purposes.

2.1.2 Our attempt to improve the key rate

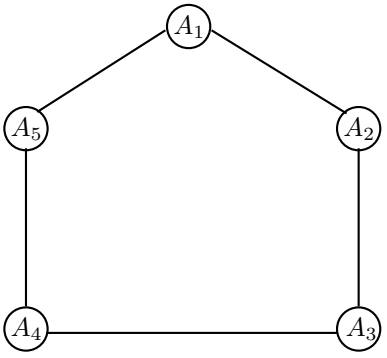

Figure 2.1: KCBS orthogonality graph for Hybrid Ekert protocol

I along with Atul and Prof. Arvind used the following contextuality pentagon to improve the key rate of the Ekert protocol. The motivation was to harness contextuality as well as entanglement to have a hybrid key distribution protocol. In the above pentagon structure, each of the corner represents a projection operator. Alice and Bob share same set of measurement operators, represented by the pentagon. The operators connected by a line are orthogonal. Our protocol goes as follows:

- Alice randomly selects a measurement operator from the the set: $\{A_i\}$
- Without loss of generality, suppose she gets A_3 in step 1. She prepares the state $|\psi_3\rangle$ such that
$$A_3 = |\psi_3\rangle\langle\psi_3| \tag{2.1}$$
- She sends the state prepared in step 2 to Bob.
- Bob performs a random measurement on the state received from Alice using either of the measurement operators from the set: $\{A_i\}$
- Now out of the following must happen:
  - if Bob carries on measurement using A_3, he is bound to get $+1$ as eigenvalue.
  - if he measures using A_2 or A_4, he gets 0.
  - else he gets 0 or 1 otherwise.
- Bob reports the operator he used in last step publicly.
- Alice notes on her notebook
  - 1, if Bob reports A_3
  - 0, if Bob reports A_2 or A_4
  - (randomly) 0 or 1 otherwise
- Alice/Bob carries on measurement in
  - X basis if she/he gets 0
  - Z basis if she/he gets 1

2.2 Bound Entanglement and Peres Conjecture

The correlation statistics predicted by quantum theory is in sharp contradiction with the theory of locality. These correlations are basically manifestations of quantum entanglement in case we are interested with violation of a Bell inequality. Though we know that the Bell inequality violation implies the presence of entanglement, it is still not known whether all entangled states can violate a Bell inequality.

In 1999, Peres conjectured that no bound entangled state can give rise to non-local correlations, which basically means bound entanglement can't be used for Bell inequality violation [Per98]. As we know that for dimensions greater than $2 \otimes 3$, entangled states with positivity under partial transpose (PPT) are bound entangled states [Per96]. For such dimensions, one can reformulate the conjecture as PPT entangled states can never give rise to nonlocality. Alternatively, one can also say that any state which leads to Bell inequality violation must be negative under partial transposition (NPT). Peres' intuition for the above conjecture was from his perception that distillability of entanglement is equivalent to nonlocality.

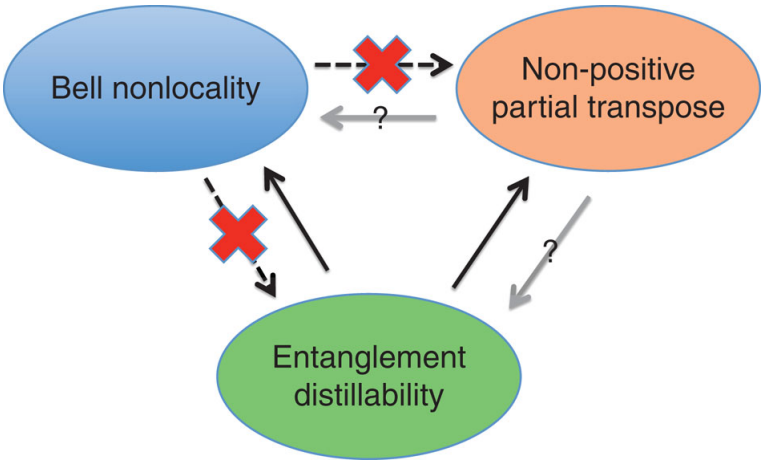

Figure 2.2: The three fundamental manifestations of quantum entanglement [VB14]

Meanwhile, non-positivity under partial transpose, distillability and Bell nonlocalities have been the three important manifestations of quantum entanglement. Hence,

it is important to understand the connection between these three foundational topics of quantum information.

2.2.1 Countering the Peres conjecture

To counter the Peres conjecture, Vertesi and Brunner constructed a quantum state ρ with the following properties [VB14]:

- ρ is positive under partial transposition. To ensure this, they constructed the ρ such that it was invariant under the partial transposition.
- In a cleverly chosen Bell type experiment, local measurements on ρ happen to violate the corresponding Bell inequality and thus ρ was Bell nonlocal.

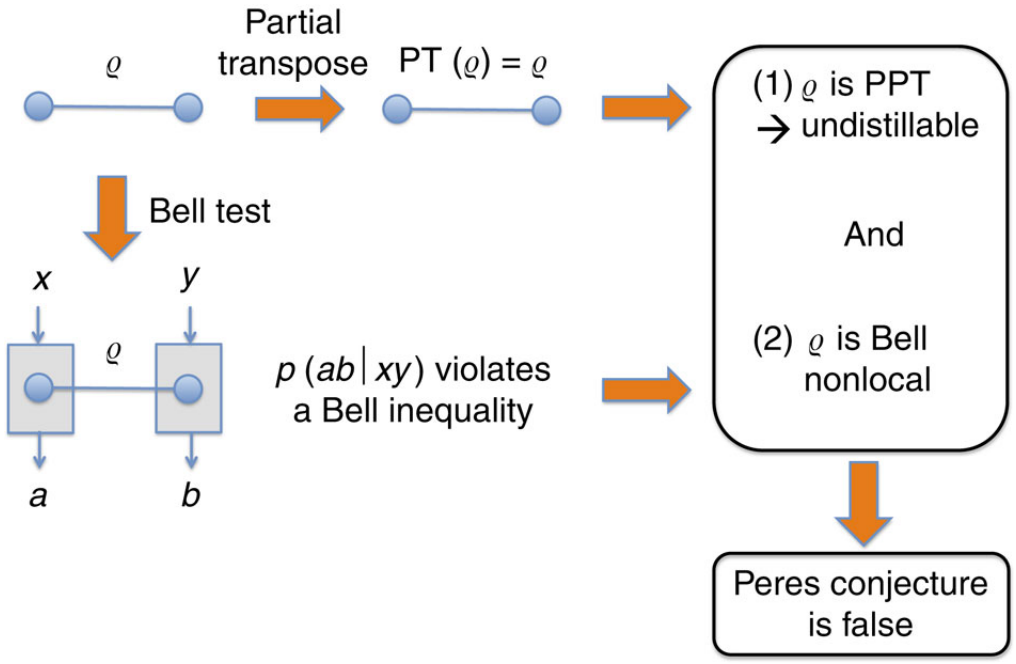

Figure 2.3: Countering the Peres conjecture [VB14]

To find out the required ρ, semidefinite programming was used [Wal11]. Specifically, following algorithm can be used.

- Generate random measurement matrices for Alice and Bob ($M_{a|x}$ and $M_{b|y}$)
- Use the measurement matrices to generate the Bell operator

$$B = \Sigma_{a,b,x,y} c_{a,b,x,y} M_{a|x} \otimes M_{b|y} \tag{2.2}$$

- Now carry on the following semidefinite programming: Maximize $Tr(B\rho)$, subject to

$$\rho \geq 0 \tag{2.3}$$

$$PT(\rho) \geq 0 \tag{2.4}$$

$$Tr(\rho) = 1 \tag{2.5}$$

- Now optimize Alice's measurement operators for fixed ρ (obtained in last step) and Bob's measurements
- Carry out a similar process for Bob
- Iterate over last three steps until you reach for the convergence of $Tr(B\rho)$

2.3 A small comment on "Improving Randomness Certification Using Sequential Measurement"

The randomness in quantum mechanics is something intrinsic to the theory and does not feature because of ignorance. It has been shown that nonlocality can be used to

certify the unpredictability present in the outcomes of certain physical process [PR], [MAG06]. This has been termed as *device independent randomness certification*. The reason for sticking with such a nomenclature is that the certification depends only on the statistical properties of the outcomes and not on the experimental set up using which they were produced.

For the multiple measurement scenario, following two comments are worth making:

- For randomness certification in the sequential Bell scenario, gradual decay of entanglement is the key aspect , which obviously projective measurements fail to achieve. This means Alice should measure her qubit once all Bobs have sequentially performed their measurements. I believe that it is possible to construct a better scenario with multiple Alices carrying on sequential measurements on their part as well.

- Nonlocality is the resource used for device independent randomness certification. Is it the only resource? Is it possible to use contextuality for device independent randomness certification? I mean violation of Bell's inequality is pivotal to device independent quantum key distribution (DIQKD). Can we use similar no-go theorems, for example KCBS to do DIQKD [HHH$^+$10]?

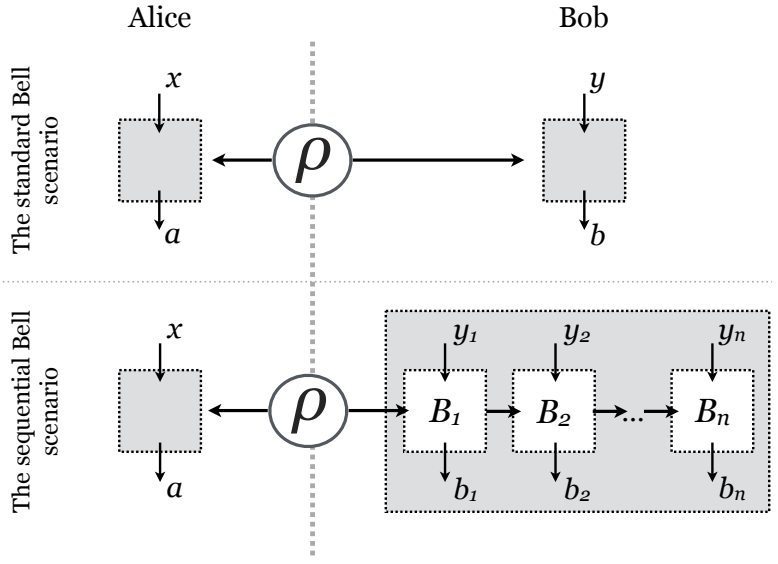

Figure 2.4: The sequential scenario
[CJA$^+$15]

Chapter 3

Conclusion and Remarks

3.1 No-Go Theorems and Device Independence

Analyzing Bell nonlocality has been prudent in the development of device independent quantum theory. For example, the *information causality* principle has emerged as a consequence of analyzing no signaling polytopes. Whether information causality turns out to be the defining principle of quantum mechanics, is still an open problem. But nonetheless, such attempts have helped in the development of device independent security proofs for quantum cryptography.

Recently, Horodecki **et. al** came up with contextuality based device independent security proof for quantum cryptography [HHH$^+$10]. There is enough evidence to extend the parallel between nonlocality and contextuality:

- CHSH vs KCBS inequalities
- Entanglement monogamy vs KCBS monogamy
- Both are capable of generating true random numbers

Thus, exploring contextuality can be pivotal in

- coming up with similar device independent physical principles
- providing evidence for information causality as the defining principle of QM

Furthermore, such attempts will be helpful to contrast the randomness generated using nonlocality to those in contextuality. This can be accomplished by exploring non-contextual polytopes and comparing the same with no signaling polytopes. Furthermore, quantifying as well as comparing randomness from these two different scenarios could be helpful.

3.2 Open Problems

The project can be proceeded further with the following open problems:

- **Separability problem :** How can one find whether a given bipartite quantum state is separable or not?
- **NPT bound entanglement problem :** The states which are positive under partial transpose, if entangled are always bound entangled. But what about NPT states?

Appendix A

Semi-Definite Programming

Semidefinite programming is a powerful technique with heavy applications in quantum information. It is useful both from an analytic as well as a computational point of view.

Definition A.1. *A semidefinite program is given by a triple* (Φ, A, B)*, such that*

- $\Phi \in T(\mathcal{X}, \mathcal{Y})$ *is a Hermiticity-preserving linear map*
- $A \in Herm(\mathcal{X})$ *and* $B \in Herm(\mathcal{Y})$ *are linear operators*

for some complex Euclidean spaces $\mathcal{X}$ *and* $\mathcal{Y}$ *[Wal11].*

Note that a mapping $\phi \in T(\mathcal{X}, \mathcal{Y})$ is called a Hermiticity preserving map if

$$\Phi(X) \in Herm(\mathcal{Y}) \quad \forall X \in Herm(\mathcal{X}) \tag{A.1}$$

Now given a triple (Φ, A, B), we can associate two optimization problems, namely Primal and Dual.

Primal Problem

The primal problem focuses on maximizing the inner product of A and X subject to some constraints. More precisely, one can state the primal problem as

$$\text{maximize} : \langle A, X \rangle \tag{A.2}$$

$$\text{subject to} : \quad \Phi(X) = B, \tag{A.3}$$

$$X \in Pos(\mathcal{X}) \tag{A.4}$$

Dual Problem

The Dual problem is about minimizing the inner product of B and Y subject to some constraints. Specifically, we can put dual problem as

$$\text{minimize} : \langle B, Y \rangle \tag{A.5}$$

$$\text{subject to} : \quad \Phi^*(Y) \geq A, \tag{A.6}$$

$$Y \in Herm(\mathcal{Y}) \tag{A.7}$$

Appendix B

Bell Violation Code

```
%
-------------------------------------------------------------------------

% Spring 2016
% Bell violation module
% Author: Kishor Bharti
% Guide: Prof. Arvind
%
-------------------------------------------------------------------------

% dimension is 3
d = 3;
% Generating Alice's and Bob measurement matrices
%
-------------------------------------------------------------------------

% M_a|x
% d1 is the number of Alice's matrices
d1 = 6;
```

```
Alice_mat =zeros(d,d,d1);
for i = 1:d1
    Alice_mat(:,:,i) = crand(d,d);
end
Alice_temp = zeros(d,d,d1);
% M_b|y
% d2 is the number of Bob's matrices
d2 = 5;
Bob_mat = zeros(d,d,d2);
for i = 1:d2
    Bob_mat(:,:,i) = crand(d,d);
end
Bob_temp = zeros(d,d,d2);

% Defining the Bell operator
% kron(Bob_mat(:,:,5), Alice_mat(:,:,1)) gives tensor
   product matrix of
% the input matrices
% Generating Coefficient matrix C
C = zeros(d1,d2);
for i = 1:d2
    C(3,i) = -1;
end
for i = 1:d1
    C(i,2) = -2;
end
C(1,3) = -1;
C(2,1) = -1;
C(3,1) = 1;
```

```
42 C(3,2) = 1;
43 C(3,3) = 1;
44 C(1,2) = 1;
45 C(2,2) = 1;
46 Bell = zeros(d^2,d^2);
47 for i = 1:d1
48     for j = 1:d2
49         Bell = Bell + C(i,j)*kron(Alice_mat(:,:,i),
               Bob_mat(:,:,j));
50     end
51 end
52
53 %
   ------------------------------------------------------------------------

54 % Semidefinite Program #1
55 %
   ------------------------------------------------------------------------

56 % the desnity matrix
57 rho = sdpvar(d^2,d^2);
58 % Positivity of partial transpose of rho
59 F = [Tx(rho,1,[d,d]) >= 0];
60 % Positivity of rho
61 F = F + [rho >= 0];
62 % Normalization
63 F = F + [trace(rho) == 1];
64 % SDP settings
65 ops = sdpsettings('verbose', 0, 'warning', 0);
```

```
% Maximizing trace(Bell*rho)
solvesdp(F, -abs(trace(Bell*rho)),ops)
% Quantifying the violation by I_Q
I_Q = real(double(trace(Bell*rho)));
rho = double(rho);

%
    ------------------------------------------------------------------------

% Semidefinite Program #2
% Optimizing Alice's matrices for fixed values of Bob's
    matrices and rho
%
    ------------------------------------------------------------------------

% Alice's matrices for optimization
Alice_new _mat = sdpvar(d,d,d1);
% Positivity
for l = 1:d1
    G = [Alice_new _mat(d,d,l) >= 0];
end
% Normalization
% This needs to be modified depending on the Bell settings
G = G + [Alice_new _mat(d,d,1) + Alice_new _mat(d,d,4) ==
    eye(d)];
G = G + [Alice_new _mat(d,d,2) + Alice_new _mat(d,d,5) ==
    eye(d)];
G = G + [Alice_new _mat(d,d,3) + Alice_new _mat(d,d,6) ==
    eye(d)];
```

```
% Defining F_a|x
for a = 1:d1
    for b = 1:d2
        Alice_temp(:,:,a) = Alice_temp(:,:,a) + C(a,b)*TrX
            (rho*kron(eye(d),Bob_mat(:,:,b)),2,[d,d]);
    end
end
I_Q_temp = 0;
for a = 1:d1
    I_Q_temp = I_Q_temp + trace(Alice_new_mat(:,:,a)*
        Alice_temp(:,:,a));
end
% SDP settings
ops = sdpsettings('verbose', 0, 'warning', 0);
% Maximizing trace(Bell*rho)
solvesdp(G,I_Q_temp,ops);
I_Q = I_Q_temp;

%%-----------------------------------------------------------
% Semidefinite Program #3
%-----------------------------------------------------------
% Optimizing Bob's matrices for fixed values of Alice's
    matrices and rho
%-----------------------------------------------------------
% Bob's matrices for optimization
Bob_new_mat = sdpvar(d,d,d2);
% Positivity
for l = 1:d2
    H = [Bob_new_mat(d,d,l) >= 0];
```

```
113 end
114 % Normalization
115 %%
116 % This needs to be modified depending on the Bell settings
117 H = H + [Bob_new_mat(d,d,1) + Bob_new_mat(d,d,3) +
        Bob_new_mat(d,d,5) == eye(d)];
118 H = H + [Bob_new_mat(d,d,2) + Bob_new_mat(d,d,4) == eye(
        d)];
119 % Defining F_a|x
120 for a = 1:d2
121     for b = 1:d1
122         Bob_temp(:,:,a) = Bob_temp(:,:,a) + C(a,b)*TrX(rho
              *kron(Bob_new_mat(:,:,b),eye(d)),1,[d,d]);
123     end
124 end
125 I_Q_temp = 0;
126 for a = 1:d2
127     I_Q_temp = I_Q_temp + trace(Bob_new_mat(:,:,a)*
          Bob_temp(:,:,a));
128 end
129 % SDP settings
130 ops = sdpsettings('verbose', 0, 'warning', 0);
131 % Maximizing trace(Bell*rho)
132 solvesdp(H,I_Q_temp,ops);
133 I_Q = I_Q_temp;
```

Bibliography

[CJA+15] Florian J. Curchod, Markus Johansson, Remigiusz Augusiak, Matty J. Hoban, Peter Wittek, and Antonio Acín, *Unbounded randomness certification using sequences of measurements*, arXiv:1510.03394 [quant-ph] (2015).

[Cla06] Lieven Clarisse, *Entanglement distillation; a discourse on bound entanglement in quantum information theory*, 2006.

[Eke91] Artur K. Ekert, *Quantum cryptography based on bell's theorem*, Phys. Rev. Lett. **67** (1991), 661–663.

[HHH+10] Karol Horodecki, Michal Horodecki, Pawel Horodecki, Ryszard Horodecki, Marcin Pawlowski, and Mohamed Bourennane, *Contextuality offers device-independent security*, 2010.

[MAG06] Ll. Masanes, A. Acin, and N. Gisin, *General properties of nonsignaling theories*, Phys. Rev. A **73** (2006), 012112.

[MBC+12] Kavan Modi, Aharon Brodutch, Hugo Cable, Tomasz Paterek, and Vlatko Vedral, *The classical-quantum boundary for correlations: Discord and related measures*, Rev. Mod. Phys. **84** (2012), 1655–1707.

[NC11] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information: 10th anniversary edition*, Cambridge University Press, 2011.

[Per96] Asher Peres, *Separability criterion for density matrices*, Phys. Rev. Lett. **77** (1996), 1413–1415.

[Per98] Asher Peres, *All the bell inequalities*, Foundations of Physics 29 (1999) 589-614, 1998.

[PR] Sandu Popescu and Daniel Rohrlich, *Quantum nonlocality as an axiom*, Foundations of Physics **24**, no. 3, 379–385.

[Sca13] Valerio Scarani, *The device-independent outlook on quantum physics (lecture notes on the power of bell's theorem)*, Acta Physica Slovaca 62, 347 (2012), 2013.

[VB14] Tamas Vertesi and Nicolas Brunner, *Disproving the peres conjecture by showing bell nonlocality from bound entanglement*, 10.1038/ncomms6297 (2014).

[Wal11] John Waltrous, *Cs 766/qic 820 theory of quantum information (fall 2011) lecture 7: Semidefinite programming*, https://cs.uwaterloo.ca/ watrous/LectureNotes.html, 2011.