NATIONAL UNIVERSITY OF SINGAPORE

Dimension Witness

Author:
Cong Wan

Supervisor:
Professor Valerio Scarani

Mentor:
Cai Yu

A thesis submitted in partial fulfillment of the
requirements for the degree of Bachelor of Science (Honours)

in the
Faculty of Science
Department of Physics

2015/2016

Abstract

Existing dimension witnesses focus on giving a lower bound to the dimension of the quantum system measured based on the observed statistics. In particular, if the dimension witness is based on Bell-inequalities, one is able to distinguish between systems that are entangled in different dimensions. However, it has been shown that violation of a qutrit bound based on the CGLMP_4 Bell-inequality can be achieved using multiple entangled qubits and sequential qubit measurements. In this report, it will be shown that a similar case happens for the dimension witness based on the CGLMP_3 Bell-inequality. We argue that such a situation makes a dimension witness trivial. A proper dimension witness without such a problem will also be presented.

Acknowledgements

I would like to thank my supervisor, Valerio, for his help in my FYP. Every important detail, from the motivation to the approach to this project has been carefully thought out by him, without which I could not have hoped to complete this project, and with minimal stress and panic. I felt well taken care of throughout my FYP thanks to his dedication as a supervisor and his clarity and skillful explanations as a teacher.

Joining Valerio's group is the best choice I could have made, not just because of FYP, but also the various enjoyable group outings and birthday surprises. I would also like to thank Valerio for his encouragements, advices on graduate schools and the opportunities he has given me to learn more.

Of course, I cannot forget to thank my mentor, Cai Yu, who has put in as much time and effort in helping me with my FYP. I want to thank him for his patience in going through with me not-so-comprehensible papers, and dealing with my laziness and reluctance to do calculations and learn matlab on my own. Almost all that I know about dimension witness, Ive learnt from him and his PhD thesis. Many of the matlab codes in the appendix (the better written ones) I've learnt from him and many of the results in the report (the correct ones) are checked by him.

I have also Jean-Daniel to thank for his explanations and suggestions for my FYP as well as short, interesting discussions on other topics. Last but not least, I would like to thank everyone in the group as well as those who have given me suggestions for this project.

Please note that, as with the report, I have probably written in a too concise manner that cannot express fully my gratitude towards all mentioned above. But I do sincerely wish to say to them: thank you!

Contents

Chapter 1

Context

In this introductory chapter, the motivation behind finding a proper dimension witness will be presented with minimal mathematical expressions. The formalities will follow in chapter 2, where Bell-inequalities will be introduced. In chapter 3, we will look at existing dimension witnesses and see why they do not constitute what we would consider a proper dimension witness. Such a proper dimension witness will be presented in chapters 4 and 5, after which I end off with some concluding statements in chapter 6.

1.1 Dimension

The dimension of a classical system refers to the number of states that the system can take. For example, the classical bit can take values 0 and 1 and is thus a system with two dimensions. An English alphabet, having 26 different states, is an example of a higher dimensional system.

In this project, we are interested in the dimensions of quantum systems. In the classical case, we are usually able to distinguish perfectly the different classical states simply by observation. In analogy, the dimension of a quantum system is defined to be the number of distinguishable, or, orthogonal states of the system.

For example, the quantum analogue of the classical bit is the quantum bit, or *qubit*, taking 2 orthogonal states, $|0\rangle$ and $|1\rangle$. By construction, any third state has to be a normalized linear combination of $|0\rangle$ and $|1\rangle$, which we can no longer distinguish perfectly from the first two states using a single quantum measurement. Therefore the qubit is a two dimensional quantum system.

In many quantum computation and information tasks, the dimension of the quantum system limits the computational power and the amount of information that can be stored.

As a simple example, consider this task: A box containing seven balls of different colours is given to Alice, who will draw a ball at random from the box. Her task is to communicate the colour of the ball drawn to Bob by preparing and sending him a quantum system. Upon receiving the quantum system, Bob can perform quantum measurements on the system to try to determine the colour of the ball drawn by Alice.

Now, if the preparation device of Alice allows her to prepare seven orthogonal quantum states, then Alice can simply encode each colour into the seven orthogonal states and upon measuring in the orthogonal basis, Bob will be able to decode the colour. However, if the preparation device of Alice is only able to prepare six orthogonal states, then the success probability of Bob will be strictly less than one. In other words, a quantum source of dimension at least seven is needed for Alice and Bob to perfectly complete this task. This simple example illustrates that the amount of information that a quantum system can encode depends on the dimension of the system.

1.2 Device-Independent Dimension Witness

Given that it may be advantageous to have higher dimensional systems, can we verify it when manufacturer claims to have constructed a high dimensional quantum system? For example, suppose the claim is that the quantum system is stored in a device on which there are two sets of buttons. We can choose to prepare the hidden quantum system in some unknown states by pressing on the first set of buttons, and make a quantum measurement on the state prepared by pressing on the second set of buttons. The outcome of the measurement is then made known say, on a display. This is illustrated in figure (Fig.) 1.1.

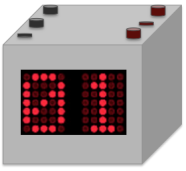


FIGURE 1.1: A manufacturer claims that a quantum system is prepared in the device. By clicking on the buttons on the left, we can choose to prepare the system in some (unknown) state. By clicking on the buttons on the right next, we choose some (unknown) measurement to perform on the system. The outcome is then displayed.

Given a general quantum state and measurement, we will be able to compute the probabilities of obtaining each outcome using quantum theory. Now, we would like to ask the reverse question: suppose we have many copies of the device so that we can obtain the probability distributions of the outcomes of the various measurements and state preparations, can we obtain any information on the dimension of the system stored in the device? Specifically, we want to give a lower bound to the dimension. This task is a form of *device-independent dimension witness*.

The term device-independent was first introduced in reference (ref.) [1], in which the authors described a way to certify security in quantum key distribution (QKD) that "needs no knowledge in the way the QKD devices work".

When queried about the properties of a quantum system, it is natural for one to try to seek out the answer by making suitable measurements on the system and interpreting the results based on knowledge of which measurement was made. For example, to find out the state of a spin-$\frac{1}{2}$ particle, one can perform tomography and measure the particle along the three orthogonal bases. If the measurement σ_z yields the outcome $+1$ with probability one, then we can conclude that the particle is in the spin up state along z-axis. The conclusion drawn in this case is contingent on one knowing the measurement carried out (σ_z) and the system that was measured (spin-$\frac{1}{2}$ particle). In a device-independent scenario, we are free from such limitations as conclusions may be drawn directly from the observed statistics.

Let us return to our example of witnessing the dimension of the quantum system stored in the device. A trivial scenario which will allow us to witness the dimension will be having four choices of state, and one four-outcome measurement on the device. If each prepared state always gives its own unique measurement outcome, then the system measured clearly has four distinguishable states and its dimension must be at least four.

The above gives a trivial example of a prepare-and-measure dimension witness, first introduced in [2]. The task was made trivial as the dimension of the system is more than or equal to the number of state choices. We are therefore allowed to use orthogonal states for each state choice and distinguish them. However, when the dimension is less than the number of state choices, it is in general non-trivial to obtain a dimension witness. Examples of such prepare-and-measure schemes can be found in ref. [2, 3].

We have discussed how the dimension of a single quantum system can be lower bounded using only the observed statistics. However, one may question the usefulness of such a scheme in two ways:

- Is it useful to find a lower bound of dimension allowed by the statistics when we know that all physical systems are essentially infinite dimensional?

- Since any single particle probability distribution can be reproduced with classical variables, why should we consider quantum systems?

To elaborate further, consider the first question. If we make measurements on a spin$-\frac{1}{2}$ particle in any directions on the Bloch sphere, we expect that the lower bound of the dimension to be at most 2. However, if instead we measure the position of the particle, the dimension will be infinite. In other words, if we include information such as a particle's position in space, then any quantum system will be infinite dimensional. Therefore, a claim to have generated a high dimensional quantum system seems to be a trivial one.

Moreover, any single particle probability distribution can be reproduced using a classical strategy. This is the issue raised in point 2. This means that whatever protocol proposed involving the use of a single quantum system could be done using classical systems, making the switch from classical to quantum systems redundant.

However, the situation changes when we consider composite quantum systems.

1.3 Entanglement and Certification

If the composite quantum system is entangled, the correlation between the subsystems cannot be achieved using classical means. Such non-classical correlations can be harnessed for various computation and communication tasks enabling us to perform tasks not only faster, but even those that are classically impossible. Quantum Key Distribution (QKD) [4] is one well-known example.

Two particles are in an entangled state if we cannot express the state as one describing each of the particles in a well-defined or pure state. On other words, the state cannot be factorized into a tensor product form, or

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$$

FIGURE 1.2: Now, a manufacturer claims that in each of the devices above, there is a qubit. Moreover, the two qubits in these two devices came from an entangled pair. By clicking on the device, we again make a quantum measurement on the quantum system in the device. Suppose after each measurement, the quantum state in the device is restored to the initial state. By performing multiple measurements and studying the statistics, we may be able to certify his claim.

where $|\psi_1\rangle$ and $|\psi_2\rangle$ are states of the two individual particles.

Entangled particles can and have been created in the lab. For example, by directing a laser beam on a non-linear crystal, one can generate photon pairs that are entangled in their linear polarization. An example of such a set up can be found in ref. [5]. In such set ups, the photons will end up in an maximally entangled state, known as the singlet state,

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

The ability to produce entangled particles is great news as it spells the possibility to physically carry out those tasks that were classically impossible. Following the logic from the previous section, we can now ask if there is a device-independent way to certify entanglement. If a manufacturer hands us two black boxes (see Fig. 1.2) in which he claims to contain one particle from an entangled pair each, can we, by pressing the buttons corresponding to quantum measurements on the particles, and studying the resultant statistics, deduce that entanglement is present?

Such a device-independent certification of entanglement exists, and is known as a Bell-test. A Bell-test involves experimental verification of the violation of Bell-inequalities [6], which are inequalities involving the statistics of the experiment. A violation of a Bell-inequality can only be achieved using entangled systems. A more detailed explanation on Bell-inequalities can be found in the next chapter. Such Bell-tests has also been experimentally demonstrated, for example in ref. [7, 8].

1.3.1 Entanglement in higher dimensions

A photon pair entangled in their linear polarization is an example of entanglement in two dimensions as there are only two orthogonal linear polarization states. In other words the state vectors describing the linear polarisation states of the photons lives in the Hilbert space $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$.

Quantum systems can also be entangled in higher dimensions, with state vectors living in $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$. For example, the state of two particles maximally entangled in d dimensions reads

$$\frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle \,.$$

Systems that are entangled in higher dimensions have also been produced in the lab. For example, in [9], entanglement in 11 dimensions was demonstrated using photons entangled in their orbital angular momentum (OAM).

1.4 Certification of Entanglement in High Dimensions

In the previous section, we have discussed and gave an example of a system entangled in high dimensions. Now, we would like a device independent way to certify it. Such a way was proposed by Brunner *et al.* in ref. [10], which was where the idea of a dimension witness was first introduced. More details on this can be found in the following chapters.

In essence, the dimension witness was based on a Bell-inequality. The maximal violation of the Bell-inequality attainable by any composite quantum systems depends on the dimension in which the system is entangled in. A sufficiently high violation value necessarily points to a system that is entangled in high dimension.

Note that it is in general non-trivial to produce particles entangled in high dimension. Given two random particles, there is no reason to belief that they are entangled at all. This is thus different from the case of the dimension of a single quantum system, where we can always think of it as being of infinite dimension. Moreover, there is legitimate reason for us to be interested in entanglement, since it allows us to accomplish tasks that cannot be done using classical resources. Therefore, dimension witnesses looking at the lower bound of entangled dimension may be more interesting then one studying the dimension of a single quantum system. However, a problem persists.

1.5 The Problem

Even though producing entangled particles is non-trivial, once we are able to produce a pair of entangled qubits, producing entangled ququarts becomes trivial! This is the consequence of isomorphism between vector spaces of the same dimension.

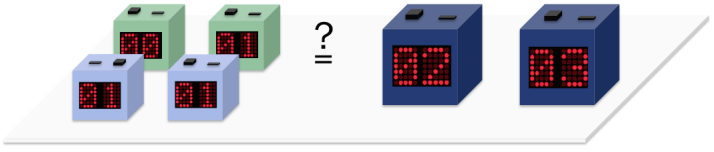


FIGURE 1.3: Each pair of the devices on the left contains an entangled qubit. The devices on the right contains a ququart each, which came from an entangled pair. Both sets of devices can be viewed as having effective entangled ququart states. However, the devices on the left are only able to make local qubit measurements.

As a result, the Hilbert space of ququart systems is equivalent to the space of two qubits, and by choosing a suitable encoding such as

$$|0\rangle \mapsto |00\rangle, |1\rangle \mapsto |01\rangle,$$
$$|2\rangle \mapsto |10\rangle, |3\rangle \mapsto |11\rangle,$$

the maximally entangled ququart state will factorise into two pairs of maximally entangled qubits:

$$\frac{|00\rangle + |11\rangle + |22\rangle + |33\rangle}{2} \mapsto \frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Physically, this means that if we have a pair of black boxes containing one particle from an entangled qubit pair each and we wish to have entangled ququarts, we can simply obtain another pair of those black boxes and taken together, we would effectively have an entangled ququart system.

Therefore, it is not difficult at all if all we are interested in is to produce systems that are entangled in high dimensions. We can simply take multiple pairs of entangled qubits. However, looking at Fig. 1.3, we do see a difference between the boxes on the left and those on the right: for the boxes on the right, the ququart system is contained in one black box and by pressing the measurement buttons, we would expect to be able to perform any general ququart measurements. However, the effective ququart system on the left is in fact two qubits contained in separate black boxes. In this case, we can still perform effective ququart measurements, by first choosing a measurement on the first box and, perhaps depending on the outcome of that measurement, choose a measurement on the second box. The outcomes of both measurements taken together will be the outcome of this effective measurement. The ququart measurements we are allowed to make is thus restricted to only *sequential local qubit measurements*.

We conclude that even though it might be trivial to obtain an entangled ququart state from entangled qubit states, it is non-trivial to perform an arbitrary ququart measurement. Hence, we finally arrive at the criteria of a proper dimension witness, which is to certify in a device independent way if a non-trivial ququart measurement has been carried out.

Unfortunately, it will be shown in subsequent chapters that the dimension witness in ref. [10] fails to do so. Our task is therefore to search for such a proper dimension witness.

Chapter 2

Formalities

As mentioned in chapter 1, dimension witness was first introduced by Brunner *et al.* in ref. [10]. There, dimension witness was defined to be a criteria on a set of joint quantum probability distributions, obtained from a standard bipartite *Bell scenario*, to lower bound the dimension of the quantum source used to generate the probablities.

In this chapter, we will first give an introduction to Bell inequalities, which is indispensable in the understanding of device-independent tasks. We will then move on to look at the formal device-independent dimension witness criteria as it was set out in ref. [10].

2.1 Bell-Inequalities

Before the development of quantum mechanics in the 1920s and 1930s, it was generally assumed that all physical properties of an object exist independent of observation. If there is a particle, the particle is somewhere in space, exhibiting a specific motion and a measurement merely allows us to obtain this information. However, with the development of quantum mechanics, there were suggestions that such properties as position and momentum of a particle does not exist prior to the measurement. Instead, the act of measuring forces the particle to take up a definite value for the measured observable.

Initially, there were many objections to this counter-intuitive view, with Einstein famously suggesting that quantum mechanics was an incomplete theory of nature [11]. However, we now know that this counter-intuitive view is indeed the correct description of how nature works thanks to the works of John Bell in the 1960s. The verification of quantum non-locality involves experiments confirming the violation of Bell-inequalities [6], which are inequalities involving the probability distributions obtained in *Bell scenarios*.

2.1.1 The bipartite Bell scenario

The Bell scenario consists of 2 parties, Alice and Bob, who are situated in separate labs. A composite quantum system will be prepared by a quantum source, one part of which is sent to Alice and the other to Bob. Alice and Bob then each chooses a measurement to make on their part of the quantum system. Alice's measurement is denoted by $x \in X = \{0, 1, ..., m_a\}$, and each measurement will give M_a possible outcomes, denoted by $a \in A = \{0, 1, ..., M_a\}$. Bob's measurement and outcome are denoted by $y \in Y = \{0, 1, ..., m_b\}$ and $b \in B = \{0, 1, ..., M_b\}$ respectively.

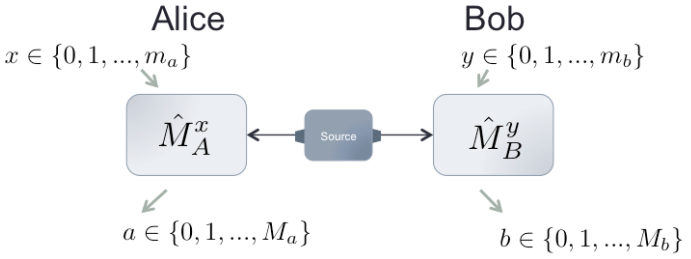


FIGURE 2.1: The bipartite Bell scenario.

Despite being spatially separated, the measurement outcomes of Alice and Bob may be correlated if the shared quantum state was entangled. In such cases, the probability of Alice obtaining outcome a and Bob obtaining outcome b when they have made measurements x and y, denoted $P(a, b|x, y)$, is such that $P(a, b|x, y) \neq P(a|x, y)P(b|x, y)$.

2.1.2 Bell-inequalities as facets of the LV polytope

The types of correlations that can naturally occur between 2 non-communicating and spatially separated parties such as Alice and Bob in a Bell scenario must satisfy the *no-signalling* criteria.

Definition 2.1. A set of probability distributions $P_{\mathcal{X},\mathcal{Y}} = \{P(a, b|x, y) : a \in A, b \in B, x \in X, y \in Y\}$ is said to be *no-signalling* if it satisfies

$$\sum_b P(a, b|x, y) = \sum_b P(a, b|x, y') \equiv P(a|x), \forall x \in X, \forall y, y' \in Y, \tag{2.1}$$

$$\sum_a P(a, b|x, y) = \sum_a P(a, b|x', y) \equiv P(b|y), \forall x, x' \in X, \forall y \in Y. \tag{2.2}$$

Intuitively, if Alice and Bob are not communicating, the output of Alice should not depend on the input of Bob. In other words, Bob cannot hope to communicate any information to Alice by affecting her output via his input. This is precisely what the above equation says.

The classical assumption that the properties of a system exist independent of measurement and that the effects of an event is only restricted to the point in space at which the event took place is termed as *local-realism*. Under such assumptions, the correlations attainable between two parties can be explained using the *local-variables* model.

Definition 2.2. A set of $P(a,b|x,y)$s can be explained by the *local-variables* model if it can be written in the form

$$P(a,b|x,y) = \sum_{\lambda} P(\lambda)P(a|x,\lambda)P(b|y,\lambda), \tag{2.3}$$

where λ is a local hidden-variable shared between Alice and Bob, with a probability distribution given by $P(\lambda)$.

The local-variables (LV) model is a precise way to describe the local realism assumption. For example, in a bipartite Bell scenario, when we assume that the results of Alice's and Bob's measurements on the quantum particles they receive are predetermined, we are essentially assuming that upon leaving the source, the pair of particles agrees on a list of outputs for each measurement setting:

$$\lambda = \{a_0, a_1, ..., a_{m_a}; b_0, b_1, ..., b_{m_b}\}.$$

Each pair of particles, upon leaving the source, can get a different list of instructions λ, drawn randomly from some set with the probability distribution given by $P(\lambda)$. In this case, the output of Alice or Bob is fully determined by λ and $P(a|x,\lambda) = \delta_{a,a_{x|\lambda}}$, where $a_{x|\lambda}$ is the instructed output for the setting x contained in λ. Similarly for Bob, $P(b|y,\lambda) = \delta_{b,b_{y|\lambda}}$. Therefore, we have

$$P(a,b|x,y) = \sum_{\lambda} P(\lambda)\delta_{a,a_{x|\lambda}}\delta_{b,b_{y|\lambda}},$$

which is in the same form as the LV model. In a LV model, correlations observed between the outputs of Alice and Bob is due to the shared variable λ. The scenario described above in which λ determines a and b uniquely is called a deterministic model. The LV model allows for more general strategies in which λ only determines the distributions, $P(a|x,\lambda)$ and $P(b|y,\lambda)$ of a and b. However, it can be shown [12] that each LV model can also be explained using a deterministic model which will result in the same $P_{\mathcal{X},\mathcal{Y}}$.

Depending on the underlying model, each $P(a,b|x,y)$ in $P_{\mathcal{X},\mathcal{Y}}$ is subjected to a number of constraints. For example, if $P_{\mathcal{X},\mathcal{Y}}$ is to be no-signalling, then Eqn. 3 and 4 will need to be satisfied. One can show that this decreases the number of free $P(a,b|x,y)$s in $P_{\mathcal{X},\mathcal{Y}}$ from $M_aM_bm_am_b$ to $D_{NS} = m_am_b(M_a-1)(M_b-1) + m_a(M_a-1) + m_b(M_b-1)$ [12].

We can then think of each $P_{\mathcal{X},\mathcal{Y}}$ as a point parametrised by these free $P(a,b|x,y)$s lying in a high dimensional real vector space, $\mathbb{R}^{D_{NS}}$.

In addition, the set of no-signalling points is convex and has a finite number of extremal points. It thus forms a polytope embedded in $\mathbb{R}^{D_{NS}}$. The set of LV points lies within this vector space since the LV model is no-signalling by construction. As it is similarly convex, the points in the LV set form another polytope. The boundaries of a polytope are hyperplanes living in the same vector space. A simple example of a polytope in 3-dimensions is shown in Fig. 2.2.

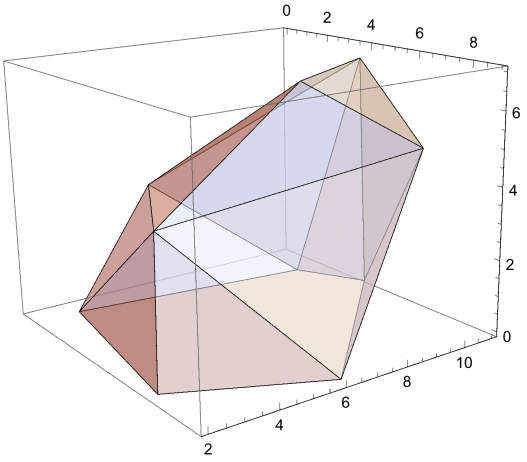


FIGURE 2.2: A polytope in $\mathbb{R}^3$. The boundaries of the enclosed region are called facets, while the facets and the enclosed points make up the polytope.

The boundaries, or facets, of the LV polytope are single out the LV set from the no-signalling set. All the probability points satisfying Eqn. 2.3 must lie within these hyperplanes. If the equation of the hyperplane is $\vec{n} \cdot P = f$ where $\vec{n} \in \mathbb{R}^D$ denotes the vector normal to the plane pointing outwards with respect to the polytope, then all probability points P belonging to the polytope must be such that

$$\vec{n} \cdot P \leq f.$$

Some of these facets are positivity facets which must be satisfied by any probability model as they ensure that the probability points are non-negative. The facets distinct to the LV polytope are called *Bell inequalities*, which are linear inequalities in the joint probability distributions.

Quantum systems satisfy the no-signalling condition Eqn. 2.1 and thus lie within the no-signalling polytope. However, violation of Bell-inequalities by quantum systems reveals that nature does not go by the LV model. We will see an example of this in the following section.

The dimension of the LV polytope and hence the form of the associated Bell-inequalities depends on the parameters m_A, m_B, M_a and M_b in the Bell scenario under consideration. For example, one of the best known Bell-inequalities, the Clauser-Horne-Shimony-Holt (CHSH) inequality [13], is the facet of the LV polytope with $m_a = m_b = M_a = M_b = 2$. Once these parameters are set, one can in principle find the facets of the LV polytope using a computer.

2.1.3 The CHSH Bell-inequality

The detailed derivation of the CHSH inequality will be omitted. However, as the inequality will be useful for subsequent discussions, it is important to at least state and understand the form of the equation.

As mentioned, the CHSH inequality deals with the scenario in which Alice and Bob each has two 2-outcome measurements. The convention is to let $a, b \in \{-1, 1\}$ and $x, y \in \{0, 1\}$. In this case, if we consider the quantum particles to share a λ at the source telling them what to output for each measurement, then the quantity

$$s = (a_0 + a_1)b_0 + (a_0 - a_1)b_1$$

can only take the values 2 or -2 in each run of the experiment. Even though the quantities in s cannot all be determined in one run, they do by assumption simultaneously exist. Over many runs of the experiment, we can determine the expectation of s. By linearity of expectation, we have

$$\begin{aligned}\langle s \rangle &= \langle (a_0 + a_1)b_0 + (a_0 - a_1)b_1 \rangle \\ &= \langle a_0 b_0 + a_1 b_0 + a_0 b_1 - a_1 b_1 \rangle \\ &= \langle a_0 b_0 \rangle + \langle a_1 b_0 \rangle + \langle a_0 b_1 \rangle - \langle a_1 b_1 \rangle \\ &= E_{00} + E_{01} + E_{10} - E_{11}\end{aligned}$$

where we define the correlation coefficients $E_{xy} \equiv P(a = b|x, y) - P(a \neq b|x, y)$. For the case in which $a, b \in \{-1, 1\}$, this is equals to $\langle a_x b_y \rangle$. Since $s = 2$ or -2, we have $\langle s \rangle < 2$ in a deterministic case. We have thus arrived at the CHSH inequality:

$$\mathcal{S} = E_{00} + E_{01} + E_{10} - E_{11} < 2. \tag{2.4}$$

While it is only shown above for deterministic cases, the CHSH inequality, being a facet of the LV polytope, is satisfied by all LV points.

In a quantum scenario, we can calculate the value of $\mathcal{S}$ by defining a Bell operator

$$\hat{\mathcal{S}} = \hat{A}_0\hat{B}_0 + \hat{A}_0\hat{B}_1 + \hat{A}_1\hat{B}_0 - \hat{A}_1\hat{B}_1 \tag{2.5}$$

where $\hat{A}_x$ and $\hat{B}_y$ are the quantum observables measured by the measurements x and y. In other words, they are hermitian operators, with eigenvalues ± 1. Since quantum theory is non-local, we would expect to find some quantum points which violate the CHSH inequality.

Indeed, an example of of such a point is achieved by considering the maximally entangled state of a qubit

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

and the observables

$$\hat{A}_0 = \hat{Z} \qquad \hat{A}_1 = \hat{X} \tag{2.6}$$

$$\hat{B}_0 = \frac{\hat{Z} + \hat{X}}{\sqrt{2}} \qquad \hat{B}_1 = \frac{\hat{Z} - \hat{X}}{\sqrt{2}} \tag{2.7}$$

where $\hat{Z}$ and $\hat{X}$ denotes the corresponding Pauli matrices. The value of $\mathcal{S}$ is then

$$\begin{aligned}\mathcal{S} &= \langle\Phi^+|\hat{\mathcal{S}}|\Phi^+\rangle \\ &= 2\sqrt{2}\end{aligned}$$

which violates the CHSH inequality. In fact, $2\sqrt{2}$ is the maximal violation achievable by quantum systems and this is known as the *Tsirelson bound* [14]:

Theorem 2.3. *Measurements on quantum systems can violate the CHSH inequality at most up to* $\mathcal{S} \leq 2\sqrt{2}$.

2.2 The Formal Dimension Witness Criteria

In many device-independent techniques, the set of joint probability distributions $\{P(a,b|x,y) : a \in A, b \in B, x \in X, y \in Y\}$ provides information on the quantum system measured without any *a priori* assumptions on the devices used for state preparation and measurement. In dimension witness, the information to be extracted is the minimum dimension of the quantum system compatible with the observed statistics.

Formally, a set of probability distributions came from a D-dimensional quantum source if each of the joint probabilities can be written in the form

$$P(a,b|x,y) = \mathrm{Tr}(\rho M_a^X \otimes M_b^Y) \tag{2.8}$$

where ρ is a density operator acting on $\mathbb{C}^D \otimes \mathbb{C}^D$ and M_a^X and M_b^Y are positive-operator valued measure (POVM) elements acting on $\mathbb{C}^D$ satisfying

$$\begin{aligned} 0 \leq M_a^X \qquad & \qquad 0 \leq M_b^Y \\ \sum_a M_a^X = \mathbb{1}_D \qquad & \qquad \sum_b M_b^Y = \mathbb{1}_D \end{aligned}$$

Following the above notation, a D-dimensional witness is defined as a linear inequality in $P(a,b|x,y)$ of the form

$$\vec{w} \cdot \vec{P} = \sum_{a,b,x,y} w_{abxy} P(a,b|x,y) \leq w_D. \tag{2.9}$$

Here, w_D is the maximal value attainable by quantum joint probabilities coming from any D-dimensional quantum systems, maximising over all possible states and measurements for a fixed $\vec{w}$. For the above inequality to be a valid dimension witness, we require further that a violation of the inequality can be achieved by quantum systems of dimensions greater than D. Hence, once a set of joint probabilities violates the D-dimensional witness, it can be certified that the quantum system producing the set is of dimension at least $D+1$.

The main challenge in any formulation of a dimension witness is thus to find a suitable $\vec{w}$ so that the maximal violation of equation (Eqn.) 2.9 is different for different dimensions. This is not a simple task in general as there is no good characterisation of the set of probabilities coming from a D-dimensional system.

Chapter 3

Dimension Witness Based on CGLMP Bell-inequalities

In this chapter an alternative motivation for dimension witness will be presented. Next, we will study two specific examples of dimension witness, and see why they are unable to fulfil this alternative motivation.

3.1 An Alternative Motivation for Dimension Witness

In ref. [10], an example of a 2-dimensional witness based on the CGLMP_3 bell inequality was given. Following this paper, other dimension witnesses to witness the dimensions of quantum systems were proposed. Some of these were based on other bell inequalities [15, 16], while others are not. For example, in [3], a prepare-and-measure scheme was introduced in which the dimension of a single quantum system can be witnessed. In [17], the authors found a dimension witness using Random Access Codes (RAC). Dimension witnesses based on Bell-inequalities are those which can distinguish between systems that are entangled in high dimensions and those that are entangled in low dimensions.

In general, the task of these dimension witnesses is to study the different sets of statistics that can be achieved by quantum systems living in Hilbert spaces of different dimensions. It was briefly mentioned in Chapter 1 that such dimension witnesses may be experimentally trivial to achieve.

We would thus like to recast dimension witness into an experimentally motivated task in which we ask the question "Given the experimental outcomes, can we certify that the experiment has genuine access to D dimensions and can perform all D-dimensional measurements?" In the previous formulation, one can in principle certify only the dimension

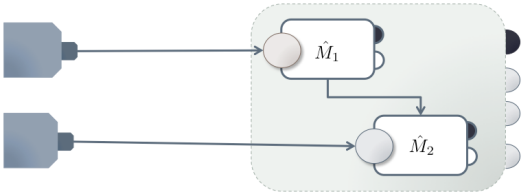


FIGURE 3.1: Demonstrating ququart measurements: An experiment which can perform all possible measurements on a ququart state has genuine access to dimension 4. However, measurements involving only sequential qubit measurements as in this figure can be trivially done using qubit set-ups.

of the quantum source used in an experiment. However, we are now also interested in the types of unitary operations carried out in the experiment.

The reason for this consideration is the realization that what sets the level of sophistication of two experiments apart is not the dimension *per se* of the quantum systems produced; if an experiment can produce a pair of entangled qubits, it can produce two pairs, giving a composite ququart system effectively. However, using the same experimental devices, such an experiment can only output probabilities resulting from *sequential qubit measurements*. In other words, the measurement operators M_a^x and M_b^y in Eqn. 2.8 can be factorised into $M_a^x = M_{a_1}^{x_1} \otimes M_{a_2}^{x_2}$, where $M_{a_1}^{x_1}$ and $M_{a_2}^{x_2}$ are operators acting on $\mathbb{C}^2$. Thus, what genuinely makes one experiment superior over another is, in addition to producing higher dimensional quantum systems, the experiment can also perform unitary operations which can transform a quantum system into any coherent superposition of states in the Hilbert space.

Therefore, it is desirable for a dimension witness to be a criteria on experimental outcomes which once satisfied, it is guaranteed that the same outcomes cannot be achieved using alternative set ups involving quantum systems of dimensions $D' \leq D$ and devices which are only capable of performing unitary operations on $\mathbb{C}^{D'}$.

This poses a problem to dimension witnesses of the form in Eqn. 2.9. If the upper bound w_D can be achieved using factorisable states and measurements, it will imply that an experiment does not need nontrivial high dimensional measurements to violate the bound. We will show that this is indeed the case for two examples of dimension witnesses based on the Collins-Gisin-Linden-Massar-Popescu (CGLMP) family of Bell inequalities.

3.2 The CGLMP Bell-Inequalities

The inequalities we are interested in is the CGLMP family of bell inequalities introduced in ref. [18]. This family of inequalities is specific for the bipartite Bell scenario mentioned in section 2.1.1 with $m_A = m_B = 2$ and for an arbitrary number of outcomes, $M_a = M_b = d$. The CGLMP_3 inequality has been independently found in [19].

Using a similar form as it appears in ref. [20], a CGLMP_d bell inequality reads

$$\langle \mathcal{I}_d, \mathcal{P} \rangle - 2 \leq 0 \tag{3.1}$$

$$\text{where } \mathcal{I}_d = \left(\begin{array}{c|c} \mathrm{J}_d & \mathrm{J}_d^T \\ \hline \mathrm{J}_d^T & \text{-}\mathrm{J}_d^T \end{array} \right) \tag{3.2}$$

Here, J_d is an upper triangular matrix with entries 1, $\mathcal{P}$ is the probability matrix and $\langle \cdot, \cdot \rangle$ denotes the sum of term by term multiplication of the two matrix arguments.

The probability matrix $\mathcal{P}$ is a matrix containing all the joint probabilities $P(a, b|x, y)$:

$$\mathcal{P} = \left(\begin{array}{c|c} \mathrm{P}^{00} & \mathrm{P}^{01} \\ \hline \mathrm{P}^{10} & \mathrm{P}^{11} \end{array} \right) \tag{3.3}$$

$$\text{with } (P^{xy})_{ab} = P(a-1, b-1|x, y) \tag{3.4}$$

The maximal possible violation of the CGLMP_d inequality Eqn. 3.1 by any quantum state $\rho \in \mathbb{C}^D \otimes \mathbb{C}^D$ depends on the dimension D. Therefore, the upper bound of the maximal violation by a quantum system living in $\mathbb{C}^D \otimes \mathbb{C}^D$ can serve as a D-dimensional witness.

3.3 2-Dimensional Witness Based on CGLMP_3 Inequality

In the CGLMP_d scenario, the number of free parameters needed to specify a no-signalling point is $4d(d-1)$. Thus, for $d = 3$, the no-signalling polytope lies in a 24 dimensional real vector space. Fortunately, by performing a classical processing on the outcomes using a method specified in ref. [21], we can project the probability points onto a two dimensional slice of the polytope, simplifying the geometry of the problem.

The points on this two dimensional slice are parametrised by two parameters, $C(\mathcal{P})$ and $D(\mathcal{P})$. $C(\mathcal{P})$ is the violation of the CGLMP_3 inequality Eqn. 3.1, with $d = 3$, while

$$D(\mathcal{P}) = -\sum_{x,y=0}^{1} \sum_{k=0}^{2} P(a = k, b = k - 1 - (x-1)(y-1)|x, y). \tag{3.5}$$

For any probability point $\mathcal{P}$ lying in the original polytope, the projected point on the two dimensional slice of the polytope will retain the same values of $C(\mathcal{P})$ and $D(\mathcal{P})$. The region accessible by quantum resources as well as qubit systems were found in ref. [10] and the results are shown in Fig. 3.2. The red curve in the figure bounds the region accessible to qubit systems, thus acting as a 2-dimensional witness.

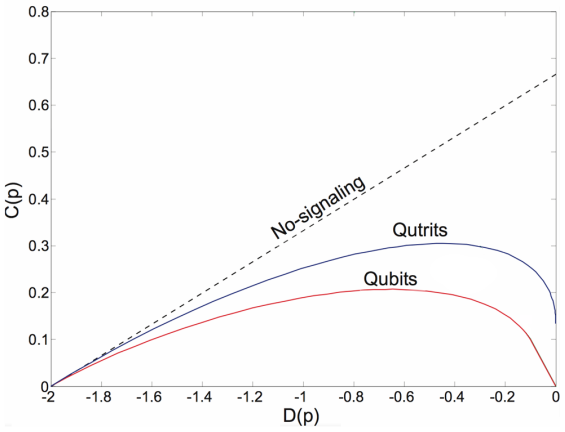


FIGURE 3.2: Given any composite quantum system ρ and measurements $\{M_a^x : x \in \{0,1\}, a \in \{0,1,2\}\}$ for Alice and $\{M_b^y : y \in \{0,1\}, b \in \{0,1,2\}\}$ for Bob, we will be able to compute the probability vector $\mathcal{P}$ using Eqn. 2.8. We can then locate this probability point in the above figure after computing its $C(\mathcal{P})$ and $D(\mathcal{P})$ values. If the point lies beyond the qubit bound, we can conclude that ρ is a density operator acting on a $\mathbb{C}^D \otimes \mathbb{C}^D$ Hilbert space, with $D > 2$.

Moreover, since only entangled quantum systems violate Bell-inequalities, this dimension witness based on the CGLMP_3 inequality, is able to distinguish quantum systems entangled in dimension 3 or above from entangled qubits.

3.4 3-Dimensional Witness Based on CGLMP_4 Inequality

Using a method similar to that by Moroder *et al.* [22], the amount of violation of the CGLMP_4 inequality has been found to be a dimension witness [23]. The negativity of a state is a measure of entanglement [24]. For an entangled qudit living in $\mathbb{C}^D \otimes \mathbb{C}^D$, the maximum negativity attainable depends on the dimension, D according to

$$\mathcal{N}(\rho) = \frac{||\rho^{T_A}|| - 1}{2} \leq \frac{D-1}{2}$$

In addition, one can find a lower bound of the minimum negativity necessary for any CGLMP_4 violation by solving a semi-definite program [25]. By comparing the lower bound obtained with the maximum negativity achievable by any states of dimension D, a dimension witness is obtained. The result is shown in Fig. 3.3 [23].

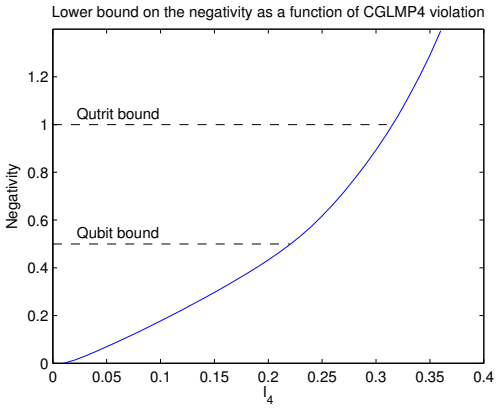


FIGURE 3.3: Lower bound on negativity against observed CGLMP_4 violation. A CGLMP_4 violation of $I_4^{(3)} = 0.315$ requires a minimum negativity of 1, which is the maximum negativity of an entangled qutrit state. Hence, any CGLMP_4 violation greater than $I_4^{(3)}$ indicates the presence of an entangled quantum system of dimension at least 4.

In particular, the upper bound of the maximal violation of the CGLMP_4 inequality by entangled qutrits is around $I_4^{(3)} = 0.315$. This thus gives a 3-dimensional witness

$$\langle I_4, \mathcal{P} \rangle - 2 \leq I_4^{(3)}.$$

In other words, any violation of the CGLMP_4 inequality above $I_4^{(3)}$ certifies the presence of entangled systems of dimension at least four.

3.5 Failure to satisfy Alternative Criteria

In section 3.1, we have seen an alternative motivation for Dimension Witness (DW), that is to certify the ability to perform arbitrary measurements on a Hilbert space of some high dimensions. In other words, we hope that the following relation holds:

satisfy DW for qu*d*its $\Rightarrow$ ability to perform arbitrary measurements on $\mathbb{C}^d \otimes \mathbb{C}^d$.

However, satisfying the CGLMP_3 and CGLMP_4 dimension witness for qutrits and ququarts respectively given in the previous sections *does not* require one to perform non-trivial measurements on high dimensional systems, as the same violation can be achieved using only qubit sources and qubit measurements.

3.5.1 Violating CGLMP_4 DW using qubits

First, we shall look at the DW based on CGLMP_4.

3.5.1.1 Maximal violation of CGLMP$_4$ using ququarts

The maximal violation of the the CGLMP$_d$ inequality allowed by quantum theory can be achieved using qu*d*its and projective qu*d*it measurements. Therefore, some composite ququart state, which we will call the maximal violation state (MVS), will be able to reach the maximal violation of the CGLMP$_4$ inequality.

The corresponding optimal measurement settings are conjectured in ref. [26]. In fact, this set of measurements is optimal for a wide class of states, including both the maximally entangled state (MES) and the MVS.

These measurement bases, labelled A_0 and A_1 for Alice and B_0 and B_1 for Bob, are:

$$A_X = \{|\Psi_x(a)\rangle\}_{a=0}^{d-1} \qquad |\Psi_x(a)\rangle = \sum_{k=0}^{d-1} \frac{\mathrm{e}^{i\frac{2\pi}{d}ak}}{\sqrt{d}} \mathrm{e}^{ik\phi_x} |k\rangle, \tag{3.6}$$

$$B_Y = \{|\Phi_y(b)\rangle\}_{b=0}^{d-1} \qquad |\Phi_y(b)\rangle = \sum_{k=0}^{d-1} \frac{\mathrm{e}^{-i\frac{2\pi}{d}bk}}{\sqrt{d}} \mathrm{e}^{ik\theta_y} |k\rangle. \tag{3.7}$$

The choice of phases θ and ϕ are

$$\phi_0 = 0, \phi_1 = \frac{\pi}{d}, \text{and } \theta_0 = -\frac{\pi}{2d}, \theta_1 = \frac{\pi}{2d}.$$

The details of how these optimal measurements are obtained is not important for us and will be omitted. Only the form of these measurements is of interest as they can be factorised into qubit measurements under a suitable choice of encoding, which we will see in the next section.

The violation value of the CGLMP$_d$ inequality by a given composite qu*d*it state, $\rho \in \mathbb{C}^d \otimes \mathbb{C}^d$, using these measurements can then be obtained by taking the trace $\mathrm{Tr}(\rho\mathcal{B})$, where $\mathcal{B}$ is the Bell operator defined as

$$\mathcal{B} = \sum_{a,b,x,y} C_{abxy} \Pi_X(a) \otimes \Pi_Y(b). \tag{3.8}$$

Here, we have $\Pi_X(a) = |\Psi_x(a)\rangle\langle\Psi_x(a)|$ and $\Pi_Y(b) = |\Phi_y(b)\rangle\langle\Phi_y(b)|$, and C_{abxy} is the Bell coefficient of $P(a,b|x,y)$ in Eqn. 3.1. As these measurements are conjectured to be optimal, the maximal violation allowed by quantum theory can thus be obtained by finding the maximal eigenvalue of $\mathcal{B}$ and the corresponding eigenstate will be the MVS.

For $d = 4$, the maximal violation is $I_4^* \approx 0.364762$ [27]. Surprisingly, this maximal violation is not achieved by the MES even though it was widely believed that entanglement should result in higher nonlocality.

The violation by the MES, $|\psi_{MES}\rangle = \frac{1}{2}(|00\rangle + |11\rangle + |22\rangle + |33\rangle)$, using the same measurement settings can be calculated from $I_4^{MES} = \langle\psi_{MES}|\mathcal{B}|\psi_{MES}\rangle$. The MES also gives a high violation of $I_4^{MES} = 0.336091$. Recall that the DW bound for qutrits from section 3.4 is $I_4^{(3)} = 0.315$. Hence, both the MVS and the MES satisfy the DW for ququarts as expected. Now, we will show that satisfying this DW does not require one to perform non-trivial ququart measurements. We will do this by demonstrating a case in which performing sequential qubit measurements on two pairs of maximally entangled qubits allows one to reach the same violation value of the ququart MES.

3.5.1.2 Achieving the MES violation

Recall from section 1.5 that as the Hilbert space of ququarts is isomorphic to the Hilbert space of two qubits, any ququart state can be written as a composite qubit state after choosing a suitable encoding. For example, with the standard binary encoding

$$\begin{aligned} |0\rangle_A \mapsto |00\rangle_{A_1,A_2}, |1\rangle_A \mapsto |01\rangle_{A_1,A_2}, \\ |2\rangle_A \mapsto |10\rangle_{A_1,A_2}, |3\rangle_A \mapsto |11\rangle_{A_1,A_2}, \end{aligned} \tag{3.9}$$

the ququart MES factorises into two pairs of maximally entangled qubits:

$$(|00\rangle + |11\rangle + |22\rangle + |33\rangle)_{A,B} \mapsto (|00\rangle + |11\rangle)_{A_1,B_1} \otimes (|00\rangle + |11\rangle)_{A_2,B_2} \tag{3.10}$$

omitting normalisation.

In other words, sending one part of a maximally entangled ququart to Alice and the other to Bob can also be seen as sending 2 pairs of maximally entangled qubits, with one qubit from each pair being sent to Alice and the other to Bob. We will label these sub-systems as A_1, A_2 and B_1, B_2. This can be trivially achieved by using a quantum source that can produce pairs of qubits in any coherent superposition.

Furthermore, using the same binary encoding, the optimal measurements in Eqn. 3.6 and 3.7 for Alice and Bob factorise into tensor products of operators acting on the sub-systems A_1, A_2 and B_1, B_2 of Alice and Bob respectively.

From Eqn. 3.6, for $d = 4$, each vector in the measurement basis is

$$|\Psi_X(a)\rangle = \frac{1}{2}(|0\rangle + \omega|1\rangle + \omega^2|2\rangle + \omega^3|3\rangle),$$

where $\omega = \mathrm{e}^{i(\frac{2a\pi}{d}+\phi_X)}$. Using the same encoding as the MES, each of these vectors factorises:

$$
\begin{aligned}
|\Psi_X(0)\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{i(2\phi_X)}|1\rangle)_{A_1} \otimes \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{i(\phi_X)}|1\rangle)_{A_2}, \\
|\Psi_X(1)\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{e}^{i(2\phi_X)}|1\rangle)_{A_1} \otimes \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{i(\frac{\pi}{2}+\phi_X)}|1\rangle)_{A_2}, \\
|\Psi_X(2)\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{i(2\phi_X)}|1\rangle)_{A_1} \otimes \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{e}^{i(\phi_X)}|1\rangle)_{A_2}, \\
|\Psi_X(3)\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{e}^{i(2\phi_X)}|1\rangle)_{A_1} \otimes \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{e}^{i(\frac{\pi}{2}+\phi_X)}|1\rangle)_{A_2}.
\end{aligned}
$$

Moreover, the vectors of A_1 form a valid measurement basis $\sigma_{A_1} = \{|0\rangle \pm \mathrm{e}^{i(2\phi_X)}|1\rangle\}$ and the vectors of A_2 form 2 measurement bases $\sigma_{A_2|+} = \{|0\rangle \pm \mathrm{e}^{i(\phi_X)}|1\rangle\}$ and $\sigma_{A_2|-} = \{|0\rangle \pm \mathrm{e}^{i(\frac{\pi}{2}+\phi_X)}|1\rangle\}$, separated according to the outcome of the first measurement.

This implies that Alice's ququart measurement given by Eqn. 3.6 can be viewed instead as first performing a qubit measurement on A_1 then, conditioning on the outcome, a second qubit measurement on A_2. This is illustrated in Fig. 3.4.

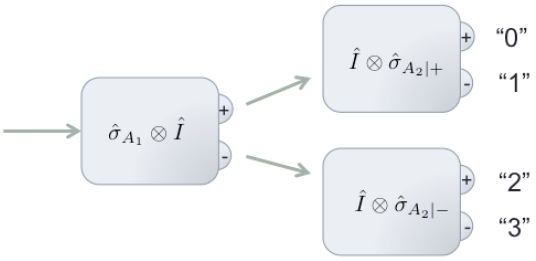


FIGURE 3.4: The measurement device first makes the measurement σ_{A_1} on A_1. If the "+" outcome is obtained, the measurement $\sigma_{A_2|+}$ will be made on A_2. The device will then output the outcome "0" if the second measurement yields "+" and "1" if the measurement yields "−". Similarly, if the outcome of the first measurement were "−", a second measurement $\sigma_{A_2|-}$ will be made on A2. The outcomes "±" will be labeled "2" and "3" respectively.

It can be easily verified that a similar factorisation happens for Bob. Using the resultant measurement scheme on the composite qubit state in Eqn. 3.10, the probabilities of obtaining any outcome $P(a, b|x, y)$ will be the same as when the optimal ququart measurement is carried out on the maximally entangled ququart. Hence, one can achieve a violation I_4^{MES} of the CGLMP_4 inequality, beating the qutrit bound in the DW, using entangled qubits and qubit measurements.

We conclude that violating this 3-dimensional witness bound does not require one to be able to perform nontrivial ququart measurements since an experiment involving only local sequential qubit measurements can also violate the bound.

Furthermore, the factorisation of the optimal measurements and MES happens to any Hilbert spaces with dimension $D = 2^k$. Hence, any DW based on CGLMP_d with $d = 2^k$ will fail to certify coherent manipulation if the MES of qudits can violate the DW bound.

3.5.2 Violating CGLMP_3 DW using qubits

That multiple pairs of entangled qubits can be used to violate the CGLMP_4 DW was first pointed out by Y. Cai in his PhD thesis [23]. However, it remained to be seen if the DW based on the CGLMP_3 inequality faces the same problem. In this section, we will see that indeed, the DW bound for $d = 3 \neq 2^k$ can be violated using multiple pairs of entangled qubits. In this case, qutrit states and measurements cannot be factorised into qubit states and sequential qubits measurements directly. Hence it is not possible to employ exactly the same strategy as the previous section to show that satisfying the DW for qutrits does not require nontrivial high dimensional measurements.

Instead, we will try to find a violation of the DW bound using sequential qubit measurements on multiple pairs of entangled qubits, which may allow for greater violation of the CGLMP_3 inequality than that achievable by measuring only one pair of qubits. In order to do this, we will have to consider classical processing of the outcomes obtained to reduce the number of outcomes to 3.

It turns out that 3 pairs of qubits can already violate the qubit bound based on the CGLMP_3 inequality in section 3.3.

The CGLMP_3 Bell scenario involves two 3-outcome measurements each for Alice and Bob. Therefore, to compute the CGLMP_3 violation using projective measurements on the Hilbert space of three qubits, we have do a coarse-graining of the $2^3 = 8$ outcomes by grouping them into 3 groups and giving each group a new label. For example, we can label the outcomes 0 and 1 as $0'$ and $1'$, and simply group all the other outcomes, 2 to 7, together and label them as $2'$. Whenever the outcome 1 is obtained, we will output $1'$; whenever 3 is obtained, we will output $2'$ and so on. We can then proceed to check the CGLMP_3 violation using this rebelling.

Before presenting the strategy of searching for a violation, we shall first look at useful theorem, called *schmidt decomposition*.

Theorem 3.1. *Suppose $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ is a pure state of a composite system, AB. Then there exist orthonormal states $|k_A\rangle$ for system A and $|k_B\rangle$ for system B such that*

$$|\psi\rangle = \sum_{k=0}^{d-1} \lambda_k |k_A\rangle |k_B\rangle,$$

where λ_ks are non-negative real numbers satisfying $\sum_k \lambda_k^2 = 1$, known as the Schmidt co-efficients.

3.5.2.1 Optimal measurement for qu-8it MES

A possible candidate for violating the CGLMP_3 inequality is the MES of qu-8it using the optimal measurements. However, as the goal is to show a violation using pairs of entangled qubits, we need to establish that whatever composite qu-8its states and measurements we use can be factorized into composite qubits states and measurements.

As before, using the standard binary encoding, the MES will factorise into 3 pairs of maximally entangled qubits:

$$\begin{aligned}(|00\rangle + |11\rangle + |22\rangle + |33\rangle + |44\rangle + |55\rangle + |66\rangle + |77\rangle)_{A,B} \\ \mapsto (|00\rangle + |11\rangle)_{A_1,B_1} \otimes (|00\rangle + |11\rangle)_{A_2,B_2} \otimes (|00\rangle + |11\rangle)_{A_3,B_3}\end{aligned}$$

In order to factorise the measurement vectors in Eqn. 3.6 as

$$\bigotimes_{i=1,2,3} (\cos(\alpha_i)|0\rangle + \mathrm{e}^{i\beta_i} \sin(\alpha_i)|1\rangle),$$

we will need to solve some simultaneous equations. One can verify that a possible solution is such that the measurements can be carried out sequentially on the 3 qubits. The case for Alice is illustrated in Fig. 3.5. The various corresponding measurement vectors are:

$$\begin{aligned}
&\sigma_{A_1} = \{|0\rangle \pm \mathrm{e}^{i(\pi+4\phi_X)}\,|1\rangle\} \\
&\sigma_{A_2|+} = \{|0\rangle \pm \mathrm{e}^{i(2\phi_X)}\,|1\rangle\}, && \sigma_{A_2|-} = \{|0\rangle \pm \mathrm{e}^{i(\frac{\pi}{2}+2\phi_X)}\,|1\rangle\} \\
&\sigma_{A_3|++} = \{|0\rangle \pm \mathrm{e}^{i(\phi_X)}\,|1\rangle\}, && \sigma_{A_3|+-} = \{|0\rangle \pm \mathrm{e}^{i(\frac{\pi}{2}+\phi_X)}\,|1\rangle\} \\
&\sigma_{A_3|-+} = \{|0\rangle \pm \mathrm{e}^{i(\frac{\pi}{4}+\phi_X)}\,|1\rangle\}, && \sigma_{A_3|--} = \{|0\rangle \pm \mathrm{e}^{i(\frac{3\pi}{4}+\phi_X)}\,|1\rangle\}
\end{aligned}$$

3.5.2.2 Searching for violation

Starting with the qu-8it MES and the corresponding optimal measurements for violating the CGLMP_8 inequality, we can optimize over all rebelling to find the maximal violation of the CGLMP_3 violation. The matlab code for this can be found in the appendix. Basically, each rebelling corresponds to a way to rewrite the $16 * 16$ probability matrix

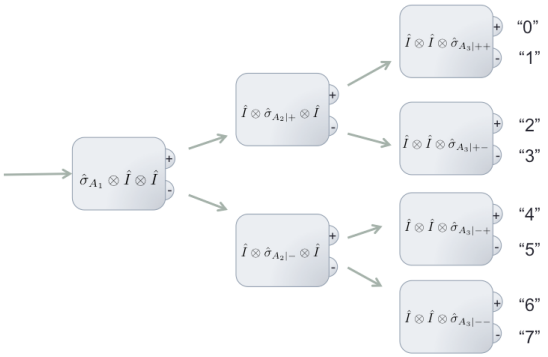


FIGURE 3.5: The measurement device first makes the measurement σ_{A_1} on A_1. If the "$\pm$" outcome is obtained, the measurement $\sigma_{A_2|\pm}$ will be made on A_2. Depending on the outcome, a third measurement will be carried out on A_3. The final output $a \in \{0, 1, ..., 7\}$ will depend on the various measurements made and outcomes obtained.

$\mathcal{P}$ in Eqn. 3.3 into a $6 * 6$ matrix $\mathcal{P}'$. The CGLMP_3 violation can then be calculated using Eqn. 3.1 with $\mathcal{P}'$ as the probability matrix. It was found that the rebelling

$$\begin{aligned} 1, 4, 7 &\mapsto 0 \\ 2, 5 &\mapsto 1 \\ 0, 3, 6 &\mapsto 2 \end{aligned}$$

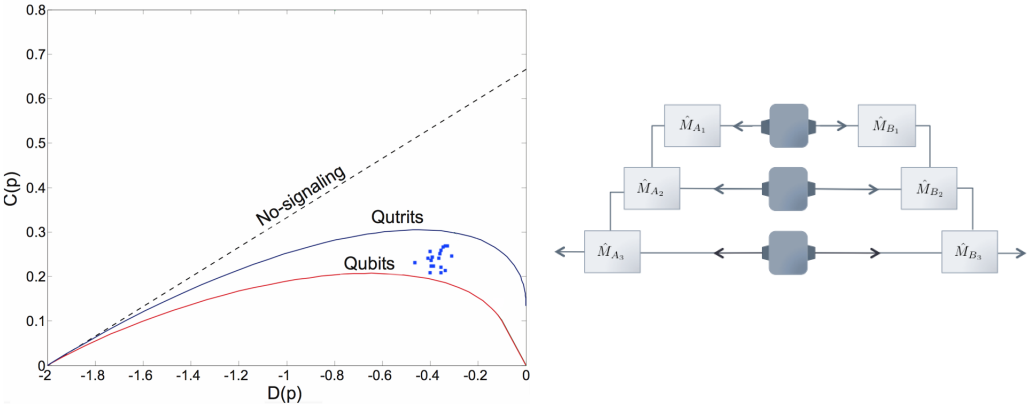
is an optimal, giving a violation of 0.2677. We can then proceed to search for a higher violation, assuming this rebelling and the optimal measurement, by optimizing over all factorisable state.

According to the Schmidt decomposition theorem, each composite qubit can be parametrised using five parameters as

$$\begin{aligned} |\psi\rangle &= \cos\theta|0_{A_1}0_{B_1}\rangle + \sin\theta|1_{A_1}1_{B_1}\rangle \\ \text{where } |0_{A_1}\rangle &= \cos\phi|0\rangle + \mathrm{e}^{-i\alpha}\sin\phi|1\rangle, |1_{A_1}\rangle = \sin\phi|0\rangle - \mathrm{e}^{i\alpha}\cos\phi|1\rangle \\ |0_{B_1}\rangle &= \cos\mu|0\rangle + \mathrm{e}^{-i\beta}\sin\mu|1\rangle, |1_{B_1}\rangle = \sin\mu|0\rangle - \mathrm{e}^{i\beta}\cos\mu|1\rangle \end{aligned}$$

where $|i_{\chi_j}\rangle$ is the Schmidt basis and $|i\rangle$ is the computational basis. A factorisable state of three pairs of qubits can thus be parametrised using 15 parameters and optimization can be carried out over all these parameters. Doing so will give us a slightly higher violation of 0.2698. One can then go on to repeat the iteration by finding a new optimal rebelling. However, the violation we achieve here already goes beyond the CGLMP_3 DW bound for qubits, which was 0.2071.

Some intermediate points with violation values between 0.2071 and 0.2698 has also been found. These points are projected onto the slice in Fig. 3.2 using the depolarization method in [21]. Fig. 3.6 shows some of these points.



(a) Projection onto slice.

(b) Sequential measurements.

FIGURE 3.6: By assuming sequential measurements on 3 pairs of qubits as in Fig. 3.6(b), one can achieve points above the qubit bound (Fig. 3.6(a)).

All of the points in Fig. 3.6 lie above the qubit bound, but can be obtained using sequential measurements on three pairs of entangled qubits. Therefore, we conclude that it does not require nontrivial measurements on dimension three or higher to satisfy the DW based on the CGLMP_3 inequality.

3.6 A Proper Dimension Witness

In the previous sections, we have seen that DWs based on the CGLMP_3 and CGLMP_4 inequalities cannot satisfy our alternative criteria since the DW bound can be surpassed using only qubit sources and sequential qubit measurements.

In order to demonstrate that the results from an experiment cannot be obtained using only entangled qubits, we would require a measurement that cannot be factorized. A prominent example of such a measurement is the *Bell measurement*, which we will study in the next chapter. A device-independent certification of a Bell measurement will constitute a proper dimension witness.

Chapter 4

Certification of Bell state measurement

A Bell state measurement is a special type of measurement in that it can result in entanglement between initially uncorrelated quantum systems. This characteristic of the Bell state measurement makes it useful in applications such as *quantum teleportation* [28] and *entanglement swapping* [29]. If the Bell state measurement in these applications could be substituted with sequential qubit measurements, then *quantum teleportation* for example, could be trivially performed in the lab. However, this is not the case. A Bell state measurement cannot be replicated using only local qubit measurements. This is precisely what we mean by a non-trivial measurement in high dimension.

In this chapter, a protocol to certify Bell state measurement would be proposed. First, we will study what a Bell state measurement is.

4.1 Bell State Measurement

A Bell state measurement on a composite qubit system is a projective measurement on the four orthonormal Bell states:

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{4.1}$$

As each of these states are orthonormal, they form a set of complete basis in the four dimensional Hilbert space of composite qubits.

For a projective measurement like the Bell state measurement, if the projectors onto each measurement bases are to be factorisable, we would be able to write each of the bases as a product state. The fact that all the measurement bases of the Bell state measurement is entangled tells us that the Bell state measurement cannot be factorised into the form $\Pi_1 \otimes \Pi_2$, where Π_1 and Π_2 are projectors on qubit spaces. For example, the equation

$$\begin{aligned}|\Phi^+\rangle\langle\Phi^+| &= \frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|) \\ &= \frac{1}{\sqrt{|a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2}}(a_1|0\rangle\langle 0| + a_2|0\rangle\langle 1| + a_3|1\rangle\langle 0| + a_4|1\rangle\langle 1|) \\ &\otimes \frac{1}{\sqrt{|b_1|^2 + |b_2|^2 + |b_3|^2 + |b_4|^2}}(b_1|0\rangle\langle 0| + b_2|0\rangle\langle 1| + b_3|1\rangle\langle 0| + b_4|1\rangle\langle 1|)\end{aligned}$$

has no solutions for the unknowns $\{a_i, b_i : i \in 1, 2, 3, 4\}$. This follows immediately from the fact that the state $|\Phi^+\rangle$ is entangled. Since local measurements will destroy any entanglement between qubits, no sequential qubit measurements can reproduce exactly a Bell state measurement scenario.

In particular, only an entangling measurement like the Bell state measurement can result in entanglement between qubits which were originally not entangled and have not directly interacted. This is what happens in *entanglement swapping* [29].

4.1.1 Entanglement Swapping

The scenario for entanglement swapping is illustrated in Fig. 4.1. A source prepares two pairs of entangled qubits in the state $|\Phi^+\rangle$ and sends one qubit from each pair to Alice and the other to Bob. Initially, Alice and Bob will each hold two uncorrelated qubits, A_1, A_2 and B_1, B_2.

The initial state of the four qubits can be rewritten as

$$|\Phi^+\rangle_{A_1,B_1}|\Phi^+\rangle_{A_2,B_2} = \frac{1}{2}(|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle)_{A_1,A_2,B_1,B_2}$$

From this, we can see that when Bob makes a Bell state measurement on his part of the system B_1, B_2, there is an equal chance of him obtaining either of the four Bell states. In addition the resulting state of Alice's system A_1, A_2 will be in the same Bell state as B_1, B_2. Hence, entanglement between originally uncorrelated qubits was created. This

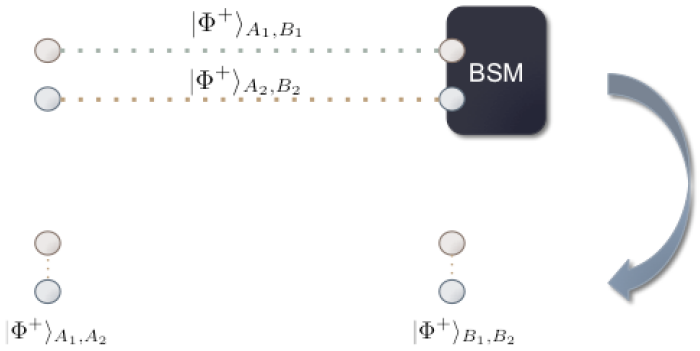


FIGURE 4.1: Entanglement swapping. A BSM by Bob (right) causes maximal entanglement in Alice's (left) particles.

characteristic of the Bell state measurement is what we will be looking out for in the protocol.

In a usual entanglement swapping scenario, the initial qubit pairs A_1, B_1 and A_2, B_2 are prepared in different Bell states. By performing a Bell state measurement followed by an unitary transformation chosen based on the Bell state measurement outcome, the entanglement between A_2, B_2 can be "swapped" to the pair A_1, A_2, hence the name "entanglement swapping".

4.2 Certifying Bell State Measurement

The procedure proposed here to certify a Bell state measurement is similar to that proposed by Rabelo *et al.* in [30]. However, we will modify the tripartite procedure proposed in that paper into a bipartite one.

The general idea of the certification is to look out for the resultant entanglement in Alice's initially uncorrelated qubits A_1 and A_2 after a Bell state measurement (BSM) by Bob on his qubits, B_1 and B_2. This is exactly the case in the entanglement swapping scenario.

In order to demonstrate this in a device independent way, we would require two sub-tests:

(i) Certify that the state sent to Alice and Bob is equivalent to two pairs of maximally entangled qubits, $|\Phi^+\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2}$. This ensures that the quantum systems received by Alice and Bob comprises of two uncorrelated subsystems each.

(ii) Certify that maximal entanglement between A_1 and A_2 is created after the BSM by Bob.

4.2.1 Test (i): Verifying presence of 2 singlets

The goal of this first sub-test is to certify that the state sent to Alice and Bob is equivalent to $|\Phi^+\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2}$ device independently. The idea of testing the quantum state in a device independent way is not new, and is in fact called *self-testing* [31] of state. The first example of self-testing is that of the state $|\Phi^+\rangle$.

In section 2.1.3, we have seen that with a suitable choice of measurements, the state $|\Phi^+\rangle$ can reach the maximal violation of the CHSH inequality given by the Tsirelson bound. In fact, we can obtain the same violation by appending additional degrees of freedom to the state $|\Phi^+\rangle\langle\Phi^+|_{AB}$ and performing identity measurements on these. Indeed, for any state ρ_{AB},

$$\begin{aligned} P(a,b|x,y) &= \mathrm{Tr}(E_x^a \otimes E_y^b \rho_{AB}) \\ &= \mathrm{Tr}((E_x^a \otimes \mathbb{1}'_A) \otimes (E_y^b \otimes \mathbb{1}'_B)\rho_{AB} \otimes \sigma_{A'B'}). \end{aligned}$$

As $\mathcal{S}$ is a linear function of the $P(a,b|x,y)$s, states capable of obtaining the same $P(a,b|x,y)$ will be achieve the same $\mathcal{S}$ value.

In fact, any bipartite state $\tilde{\rho}_{AB}$ that is equivalent to $|\Phi^+\rangle$ up to local isometries will be able to achieve the same violation. In other words, if there exist a local isometry $\mathcal{I} = \mathcal{I}_{AA'} \otimes \mathcal{I}_{BB'}$ that can map $|\Phi^+\rangle\langle\Phi^+|$ from $\tilde{\rho}_{AB}$ onto an appended 2-qubits ancilla system, $\sigma_{A'B'}$:

$$\mathcal{I}(\tilde{\rho}_{AB} \otimes \sigma_{A'B'})\mathcal{I}^\dagger = \rho_{AB}^{junk} \otimes |\Phi^+\rangle\langle\Phi^+|_{A'B'},$$

then we will be able to achieve $\mathcal{S} = 2\sqrt{2}$ by simply making the necessary measurements on A' and B' and identity measurements on A and B.

However, it is not clear if $\mathcal{S} = 2\sqrt{2}$ also implies that the state measured must be equivalent to $|\Phi^+\rangle$. The answer, according to self-testing, turns out to be yes [32].

Theorem 4.1. *If a CHSH test yields $\mathcal{S} = 2\sqrt{2}$ exactly, then the state is equivalent, up to local isometries, to $|\Phi^+\rangle$ and the measurements are the corresponding Pauli matrices.*

More recently, a criteria on $P(a,b|x,y)$ for the self-testing of $|\Phi^+\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2}$ has also been found [33]. This *double CHSH* test is what we will employ as our test (i).

In the double CHSH test, Alice and Bob will each have four 4-outcome measurement settings, $x, y, a, b \in \{0,1,2,3\}$. The idea of the test is to look at each of these measurements and outcomes as if they represent the measurements and outcomes on two subsystems A_1, A_2 and B_1, B_2 for Alice and Bob respectively. This is illustrated in Fig. 4.2.

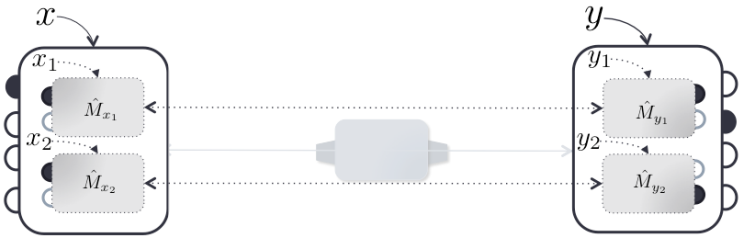


FIGURE 4.2: Double CHSH test. Each measurement of Alice and Bob will be interpreted as local measurements on 2 subsystems. The inputs and outputs will be interpreted as in the text. For example, when the measurement device on the right gives the first outcome, or $a = 0$, we will interpret it as $a_1 = 0$ and $a_2 = 0$.

We will interpret the outcomes and settings as

$$a = 2a_1 + a_2 \qquad x = 2x_1 + x_2$$
$$b = 2b_1 + b_2 \qquad y = 2y_1 + y_2$$

For example, the case in which $x = 1$ and $a = 3$ will be interpreted as Alice measuring A_1 in $x_1 = 0$ and A_2 in $x_2 = 1$ and obtaining the outcomes $a_1 = 1$ and $a_2 = 1$.

In order to certify that the state is equivalent to $|\Phi^+\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2}$, Alice and Bob will need to observe the following results:

$$\mathcal{S}_{A_1B_1|x_2=0} = 2\sqrt{2} \qquad \mathcal{S}_{A_1B_1|x_2=1} = 2\sqrt{2} \tag{4.2}$$
$$\mathcal{S}_{A_2B_2|x_1=0} = 2\sqrt{2} \qquad \mathcal{S}_{A_2B_2|x_1=1} = 2\sqrt{2}. \tag{4.3}$$

In other words, four CHSH tests need to be carried out, with two on A_1 and B_1, conditioned on Alice's input for A_2, and two on A_2 and B_2 conditioned on Alice's input for A_1.

Explicitly, in every run of the experiment, Alice and Bob will record down the outcomes and measurements made as $(a_1, a_2, b_1, b_2; x_1, x_2, y_1, y_2)$. To obtain the value of $\mathcal{S}_{A_1B_1|x_2=0}$ for example, they will filter out the results for which $x_2 = 0$, rewrite the data by ignoring the values for A_2 and B_2:

$$(a_1, a_2, b_1, b_2; x_1, 0, y_1, y_2) \mapsto (a_1, b_1; x_1, y_1)$$

and carry out the CHSH test for A_1 and B_1 using these data.

As with the self-testing of $|\Phi^+\rangle$, these results also certify that the measurements x_1, x_2, y_1, y_2 carried out are the corresponding Pauli matrices in Eqn. 2.6. The proof that this double CHSH criteria self-tests the state $|\Phi^+\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2}$ and measurements can be found in the appendix of [33].

4.2.1.1 Significance of Test (i)

From test (i), we can conclude that the state sent to Alice and Bob can be viewed as two pairs of maximally entangled qubits. By monogamy of entanglement [34], which states that if A is maximally entangled with B, then it must be uncorrelated with any other systems, we have: A_1 is uncorrelated with A_2 and B_1 is uncorrelated with B_2. Therefore, if a fifth measurement of Bob were to result in maximal entanglement in Alice's subsystems, we can certify that a BSM was carried out. This is the goal of test (ii).

It is clear that test (i) does not require non-trivial measurement on ququart systems since the required results of Eqns. 4.2 and 4.3 can be achieved by actually sending the self-tested state to Alice and Bob and making local qubit measurements on the subsystems. However, as any 2-qubit states and measurements can be viewed as ququart states and measurements by choosing an encoding, we can also use ququart systems to satisfy test (i). As an exercise, we will look at an explicit example by simply mapping the necessary 2-qubit states and measurements onto the ququart space.

We will use the inverse of the standard binary encoding in Eqn. 3.9. This will map the state $|\Phi^+\rangle_{A_1,B_1}|\Phi^+\rangle_{A_2,B_2}$ back into the maximally entangled ququart state, which is simply the reverse of Eqn. 3.10.

To achieve the maximal CHSH violation in the 2-qubits scenario, Alice and Bob need to perform local measurements on their respective subsystems chosen from the optimal CHSH measurements in Eqn. 2.6 and Eqn. 2.7 for $|\Phi^+\rangle$. For example, we can choose the following measurements for Alice:

$$x = 0 : \{\Pi^z_+ \otimes \Pi_+^{\frac{z+x}{\sqrt{2}}}, \Pi^z_+ \otimes \Pi_-^{\frac{z+x}{\sqrt{2}}}, \Pi^z_- \otimes \Pi_+^{\frac{z+x}{\sqrt{2}}}, \Pi^z_- \otimes \Pi_-^{\frac{z+x}{\sqrt{2}}}\} \mapsto \{|\Psi_0(a)\rangle\langle\Psi_0(a)| : a \in 0,1,2,3\}$$

$$\text{where } |\Psi_0(0)\rangle = c|0\rangle + s|1\rangle$$

$$|\Psi_0(1)\rangle = s|0\rangle - c|1\rangle$$

$$|\Psi_0(2)\rangle = c|2\rangle + s|3\rangle$$

$$|\Psi_0(3)\rangle = s|2\rangle - c|3\rangle$$

$$x = 1 : \{\Pi^z_+ \otimes \Pi_+^{\frac{z-x}{\sqrt{2}}}, \Pi^z_+ \otimes \Pi_-^{\frac{z-x}{\sqrt{2}}}, \Pi^z_- \otimes \Pi_+^{\frac{z-x}{\sqrt{2}}}, \Pi^z_- \otimes \Pi_-^{\frac{z-x}{\sqrt{2}}}\} \mapsto \{|\Psi_1(a)\rangle\langle\Psi_1(a)| : a \in 0,1,2,3\}$$

$$\text{where } |\Psi_1(0)\rangle = c|0\rangle - s|1\rangle$$

$$|\Psi_1(1)\rangle = s|0\rangle + c|1\rangle$$

$$|\Psi_1(2)\rangle = c|2\rangle - s|3\rangle$$

$$|\Psi_1(3)\rangle = s|2\rangle + c|3\rangle$$

$$x=2:\{\Pi_+^x\otimes\Pi_+^{\frac{z+x}{\sqrt{2}}},\Pi_+^x\otimes\Pi_-^{\frac{z+x}{\sqrt{2}}},\Pi_-^x\otimes\Pi_+^{\frac{z+x}{\sqrt{2}}},\Pi_-^x\otimes\Pi_-^{\frac{z+x}{\sqrt{2}}}\}\mapsto\{|\Psi_2(a)\rangle\langle\Psi_2(a)|:a\in0,1,2,3\}$$

$$\text{where } |\Psi_2(0)\rangle=\frac{1}{\sqrt{2}}(c|0\rangle+s|1\rangle+c|2\rangle+s|3\rangle)$$

$$|\Psi_2(1)\rangle=\frac{1}{\sqrt{2}}(s|0\rangle-c|1\rangle+s|2\rangle-c|3\rangle)$$

$$|\Psi_2(2)\rangle=\frac{1}{\sqrt{2}}(c|0\rangle+s|1\rangle-c|2\rangle-s|3\rangle)$$

$$|\Psi_2(3)\rangle=\frac{1}{\sqrt{2}}(s|0\rangle-c|1\rangle-s|2\rangle+c|3\rangle)$$

$$x=3:\{\Pi_+^x\otimes\Pi_+^{\frac{z-x}{\sqrt{2}}},\Pi_+^x\otimes\Pi_-^{\frac{z-x}{\sqrt{2}}},\Pi_-^x\otimes\Pi_+^{\frac{z-x}{\sqrt{2}}},\Pi_-^x\otimes\Pi_-^{\frac{z-x}{\sqrt{2}}}\}\mapsto\{|\Psi_3(a)\rangle\langle\Psi_3(a)|:a\in0,1,2,3\}$$

$$\text{where } |\Psi_3(0)\rangle=\frac{1}{\sqrt{2}}(c|0\rangle-s|1\rangle+c|2\rangle-s|3\rangle)$$

$$|\Psi_3(1)\rangle=\frac{1}{\sqrt{2}}(s|0\rangle+c|1\rangle+s|2\rangle+c|3\rangle)$$

$$|\Psi_3(2)\rangle=\frac{1}{\sqrt{2}}(c|0\rangle-s|1\rangle-c|2\rangle+s|3\rangle)$$

$$|\Psi_3(3)\rangle=\frac{1}{\sqrt{2}}(s|0\rangle+c|1\rangle-s|2\rangle-c|3\rangle).$$

In the above expressions, we have denoted $c=\cos\frac{\pi}{8}$ and $s=\sin\frac{\pi}{8}$ and $\Pi_\pm^{\hat{O}}$ as the projector onto the eigen-subspace of the observable $\hat{O}$ with eigenvalue ±1. The corresponding ququart measurements which the binary encoding will map to is also shown.

Similarly, for Bob, we choose:

$$y=0:\{\Pi_+^{\frac{z+x}{\sqrt{2}}}\otimes\Pi_+^z,\Pi_-^{\frac{z+x}{\sqrt{2}}}\otimes\Pi_+^z,\Pi_+^{\frac{z+x}{\sqrt{2}}}\otimes\Pi_-^z,\Pi_-^{\frac{z+x}{\sqrt{2}}}\otimes\Pi_-^z\}\mapsto\{|\phi_0(b)\rangle\langle\phi_0(b)|:b\in0,1,2,3\}$$

$$\text{where } |\phi_0(0)\rangle=c|0\rangle+s|2\rangle$$

$$|\phi_0(1)\rangle=c|1\rangle+s|3\rangle$$

$$|\phi_0(2)\rangle=s|0\rangle-c|2\rangle$$

$$|\phi_0(3)\rangle=s|1\rangle-c|3\rangle$$

$$y=1:\{\Pi_+^{\frac{z+x}{\sqrt{2}}}\otimes\Pi_+^x,\Pi_-^{\frac{z+x}{\sqrt{2}}}\otimes\Pi_+^x,\Pi_+^{\frac{z+x}{\sqrt{2}}}\otimes\Pi_-^x,\Pi_-^{\frac{z+x}{\sqrt{2}}}\otimes\Pi_-^x\}\mapsto\{|\phi_1(b)\rangle\langle\phi_1(b)|:b\in0,1,2,3\}$$

$$\text{where } |\phi_1(0)\rangle=\frac{1}{\sqrt{2}}(c|0\rangle+c|1\rangle+s|2\rangle+s|3\rangle)$$

$$|\phi_1(1)\rangle=\frac{1}{\sqrt{2}}(c|0\rangle-c|1\rangle+s|2\rangle-s|3\rangle)$$

$$|\phi_1(2)\rangle=\frac{1}{\sqrt{2}}(s|0\rangle+s|1\rangle-c|2\rangle-c|3\rangle)$$

$$|\phi_1(3)\rangle=\frac{1}{\sqrt{2}}(s|0\rangle-s|1\rangle-c|2\rangle+c|3\rangle)$$

$$y=2:\{\Pi_{+}^{\frac{z-x}{\sqrt{2}}}\otimes\Pi_{+}^{z},\Pi_{-}^{\frac{z-x}{\sqrt{2}}}\otimes\Pi_{+}^{z},\Pi_{+}^{\frac{z-x}{\sqrt{2}}}\otimes\Pi_{-}^{z},\Pi_{-}^{\frac{z-x}{\sqrt{2}}}\otimes\Pi_{-}^{z}\}\mapsto\{|\phi_2(b)\rangle\langle\phi_2(b)|:b\in 0,1,2,3\}$$

where $|\phi_2(0)\rangle = c|0\rangle - s|2\rangle$

$|\phi_2(1)\rangle = c|1\rangle - s|3\rangle$

$|\phi_2(2)\rangle = s|0\rangle + c|2\rangle$

$|\phi_2(3)\rangle = s|1\rangle + c|3\rangle$

$$y=3:\{\Pi_{+}^{\frac{z-x}{\sqrt{2}}}\otimes\Pi_{+}^{x},\Pi_{-}^{\frac{z-x}{\sqrt{2}}}\otimes\Pi_{+}^{x},\Pi_{+}^{\frac{z-x}{\sqrt{2}}}\otimes\Pi_{-}^{x},\Pi_{-}^{\frac{z-x}{\sqrt{2}}}\otimes\Pi_{-}^{x}\}\mapsto\{|\phi_3(b)\rangle\langle\phi_3(b)|:b\in 0,1,2,3\}$$

where $|\phi_0(0)\rangle = \frac{1}{\sqrt{2}}(c|0\rangle + c|1\rangle - s|2\rangle - s|3\rangle)$

$|\phi_3(1)\rangle = \frac{1}{\sqrt{2}}(c|0\rangle - c|1\rangle - s|2\rangle + s|3\rangle)$

$|\phi_3(2)\rangle = \frac{1}{\sqrt{2}}(s|0\rangle + s|1\rangle + c|2\rangle + c|3\rangle)$

$|\phi_3(3)\rangle = \frac{1}{\sqrt{2}}(s|0\rangle - s|1\rangle + c|2\rangle - c|3\rangle)$

The qubit measurements above for Alice and Bob will lead to maximal CHSH violations $\mathcal{S}_{a_i,b_i|x_{i+1}} = 2\sqrt{2}, \forall i \in \{0,1\}$ for $|\Phi^+\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2}$. Similarly, the corresponding ququart measurements will lead to maximal violations for the ququart MES.

4.2.2 Test (ii): Verifying Entanglement between A_1 and A_2

If the setting $y = 4$ of Bob were a BSM, then from section 4.1.1, A_1 and A_2 would end up in one of the entangled Bell states, depending on the outcome of the BSM. Conversely, if all CHSH tests on A_1 and A_2 conditioned on each measurement outcome of $y = 4$ give maximal violations of $\tilde{\mathcal{S}}_{A_1,A_2|b} = 2\sqrt{2}\ \forall b \in \{0,1,2,3\}$, then Bob's measurement has resulted in maximal entanglement between originally uncorrelated qubits thus certifying that $y = 4$ was a BSM.

Since test (i) certifies that each of the 4-outcome measurements $x \in \{0,1,2,3\}$ corresponds to two sequential optimal local qubit measurements on A_1 and A_2 in Eqn. 2.6, we can already use these settings for the CHSH tests on A_1 and A_2.

However, the measurements that would lead to maximal violation of the CHSH inequality, Eqn. 2.4 are different for each of the four Bell states. This problem can be resolved by noticing that using the same measurements optimal for $|\Phi^+\rangle$, the other three Bell states will maximally violate Bell inequalities of a similar form to Eqn. 2.4 which are just different linear combinations of the various E_{xy} terms. Hence, Alice would need to

compute these expressions for A_1 and A_2 for each outcome of Bob. They are

$$\begin{aligned} s_0 &= -s_3 = E_{00} + E_{01} + E_{10} - E_{11}, \\ s_1 &= -s_2 = E_{00} + E_{01} - E_{10} + E_{11}. \end{aligned} \tag{4.4}$$

For example, for $b = 0$, s_0 can be calculated as

$$\begin{aligned} s_0 &= \mathcal{E}_{00|0} + \mathcal{E}_{01|0} + \mathcal{E}_{10|0} - \mathcal{E}_{11|0} \\ \text{where } \mathcal{E}_{x_1x_2|b} &= P(a_1 = a_2|x_1, x_2, b) - P(a_1 \neq a_2|x_1, x_2, b) \\ &= P(a = 0 \text{ or } 3|x = 2x_1 + x_2, b) - P(a = 1 \text{ or } 2|x = 2x_1 + x_2, b). \end{aligned}$$

The conditioning of the probabilities on $y = 4$ is suppressed in the above expression since we are under the assumption that Bob always make this same measurement for test (ii).

It can be verified that the $(i+1)$-th Bell state in Eqn. 4.1 will give $s_i = 2\sqrt{2}$. However, since we do not know which Bell state each outcome b correspond to, Alice will need to compute all values from set $\{s_i : i = 0, 1, 2, 3\}$ for each b and keep the highest value as $\tilde{\mathcal{S}}_{A_1,A_2|b}$.

4.2.3 Remarks

In order to satisfy both tests (i) and (ii), non-trivial measurements on ququart system have to be involved. From the double CHSH criteria, we know that test (i) can be satisfied using multiple 2-qubit states and sequential qubit measurements if and only if the state is equivalent to $|\Phi^+\rangle_{A_1,B_1}|\Phi^+\rangle_{A_2,B_2}$. However, to satisfy test (ii) using the same state and measurement for Alice, a BSM by Bob has to be involved. From the discussion in section 4.1, we know that a BSM cannot be done using sequential qubit measurements.

As with test (i), test (ii) can also be satisfied using ququarts and ququart measurements. We will now complete the exercise in section 4.2.1.1 and find the necessary ququart

measurement which corresponds to $y = 4$:

$$y = 4 : \{|\Phi^+\rangle\langle\Phi^+|, |\Phi^-\rangle\langle\Phi^-|, |\Psi^+\rangle\langle\Psi^+|, |\Psi^-\rangle\langle\Psi^-|\} \mapsto \{|\phi_4(b)\rangle\langle\phi_4(b)| : b \in 0,1,2,3\}$$

$$\begin{aligned}
\text{where } |\phi_1(0)\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |3\rangle) \\
|\phi_1(1)\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |3\rangle) \\
|\phi_1(2)\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) \\
|\phi_1(3)\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle).
\end{aligned}$$

The reason for the choice of measurements x_1 and x_2 from the previous example is now clear: these are the optimal CHSH measurements for A_1 and A_2. Conditioning on Bob's outcome $b = i$, Alice will find on computing the various s_j in Eqn. 4.4, that $s_i = 2\sqrt{2}$.

Chapter 5

Deviation from Ideal

In the previous chapter, we have seen how certifying a perfect BSM serves as a DW, certifying the ability to perform non-trivial ququart measurements. However, one can rarely observe the exact statistics required for the tests in experiments due to imperfections in the measurement and state preparation devices. Therefore, it will be instructive to investigate what happens to the observed statistics when one deviates from the perfect scenario. In particular, we would like to know to what extend can the statistics be allowed to deviate from the perfect scenario before one stops certifying non-trivial ququart measurements.

A similar problem was studied in ref. [30] and it turns out that if the first step of the certification is perfect, in other words, one certifies that the state sent to Alice and Bob is $|\Phi^+\rangle_{A_1,B_1}|\Phi^+\rangle_{A_2,B_2}$ up to local isometries, then a CHSH value of

$$\tilde{\mathcal{S}}_{A_1A_2|b} \geq \sqrt{2}$$

in the second step is enough for certification.

In this chapter, we will give a proof to the above claim and look at some exercises to investigate how the observed statistics will change when the state in test (i) and BSM in test (ii) of the certification procedure differs from the ideal case.

5.1 Mixed State with Entangling Measurement

In this section, we look at what happens to the observed statistics if the state sent to Alice and Bob in the first step is two pairs of imperfect singlets and the BSM in the second step is a general entangling measurement.

Specifically, the state we consider is two pairs of Werner states

$$\rho_{A_1B_1A_2B_2} = (v|\Phi^+\rangle\langle\Phi^+| + (1-v)\frac{\mathbb{1}}{4})^{\otimes 2}, \tag{5.1}$$

which is the $|\Phi^+\rangle$ state mixed with white noise. In this case, if a CHSH test is carried out on the subsystems $\rho_{A_1B_1}$ and $\rho_{A_2B_2}$, the maximal violation we can get is clearly $\mathcal{S} = v2\sqrt{2}$ using the optimal measurements for $|\Phi^+\rangle$ since white noise will not contribute any violation.

In the second test, the BSM of Bob is replaced with a general entangled measurement, which is a projective measurement on $\{|\Psi_b\rangle : b = 0, 1, 2, 3\}$ with

$$\begin{aligned}
|\Psi_0\rangle &= \cos(\theta)|00\rangle + \sin(\theta)|11\rangle \\
|\Psi_1\rangle &= \sin(\theta)|00\rangle - \cos(\theta)|11\rangle \\
|\Psi_2\rangle &= \cos(\theta)|01\rangle + \sin(\theta)|10\rangle \\
|\Psi_3\rangle &= \sin(\theta)|01\rangle - \cos(\theta)|10\rangle.
\end{aligned} \tag{5.2}$$

Depending on the outcome $b \in \{0, 1, 2, 3\}$ of Bob's measurement, the resultant state after the measurement is given by

$$\rho_{A_1A_2B_1B_2|b} = \frac{\mathbb{1}_A \otimes |\Psi_b\rangle\langle\Psi_b|\rho_{A_1A_2B_1B_2}\mathbb{1}_A \otimes |\Psi_b\rangle\langle\Psi_b|}{\mathrm{Tr}(\mathbb{1}_A \otimes |\Psi_b\rangle\langle\Psi_b|\rho_{A_1A_2B_1B_2})}.$$

With this, we can proceed to calculate the CHSH violation by the subsystems $\rho_{A_1A_2|b}$ conditioned on the outcome of Bob. Assuming that the measurements of Alice in test (i) corresponds to the optimal measurements for CHSH violation by $|\Phi^+\rangle$, we can construct the Bell operator. For simplicity, let us consider only the $b = 0$ case. Following section 4.2.2, the bell operator in this case is given by

$$\hat{\mathcal{S}} = \hat{Z} \otimes \frac{\hat{Z} + \hat{X}}{\sqrt{2}} + Z \otimes \frac{\hat{Z} - \hat{X}}{\sqrt{2}} + \hat{X} \otimes \frac{\hat{Z} + \hat{X}}{\sqrt{2}} - \hat{X} \otimes \frac{\hat{Z} - \hat{X}}{\sqrt{2}}. \tag{5.3}$$

Finally, the CHSH violation of $\rho_{A_1A_2|b=0}$ is given by

$$\mathcal{S} \equiv \langle \hat{\mathcal{S}} \otimes \mathbb{1}_b \rangle = \mathrm{Tr}(\hat{\mathcal{S}} \otimes \mathbb{1}_b \rho_{A_1A_2|b=0}).$$

A matlab code for the above calculations has been written to find the dependence of the CHSH violation between Alices subsystems in test (ii) on the parameters v and θ. The result is

$$\mathcal{S}(v, \theta) = v^2\sqrt{2}(\sin(2\theta) + 1). \tag{5.4}$$

In the case when $v = 1$, $\theta = \frac{\pi}{4}$, we get back the ideal case and $\mathcal{S} = 2\sqrt{2}$ as expected.

5.2 Noisy BSM

In this section, we consider the case of a noisy BSM in test (ii) in which the outcomes of the measurement are mixed up.

In other words, whenever the BSM on subsystems B_1 and B_2 yields the i-th bell state, $|\psi_i\rangle$ in Eqn. 4.1, the measurement device will output the result as outcome j with probability $P_{ij} = P(b = j|\psi_i)$. For convenience, we shall let the output $b \in \{1, 2, 3, 4\}$ in this section so that P_{ij}, $i, j \in \{1, 2, 3, 4\}$ denotes the entries of the $4 * 4$ matrix, P. We shall also assume that the results in test (i) correspond to the ideal case.

In this scenario, when the measurement device outputs $b = j$, there is some probability $P(\psi_i|b = j)$ that the actual BSM yielded the state ψ_i, where

$$\begin{aligned}
|\psi_1\rangle &= |\Phi^+\rangle \\
|\psi_2\rangle &= |\Phi^-\rangle \\
|\psi_3\rangle &= |\Psi^+\rangle \\
|\psi_4\rangle &= |\Psi^-\rangle.
\end{aligned}$$

These probabilities are given by

$$\begin{aligned}
P(\psi_i|b = j) &= \frac{P(\psi_i \cap b = j)}{P(b = j)} \\
&= \frac{P_{ij}\,\mathrm{Tr}((\mathbb{1} \otimes |\psi_i\rangle\langle\psi_i|)\rho_{AB})}{P(b = j)},
\end{aligned}$$

where

$$\begin{aligned}
P(b = j) &= \sum_{i=1}^{4} P(\psi_i)P_{ij} \\
&= \sum_{i=1}^{4} \mathrm{Tr}((\mathbb{1} \otimes |\psi_i\rangle\langle\psi_i|)\rho_{AB})P_{ij},
\end{aligned}$$

and ρ_{AB} is the state of Alice and Bob's system after test (i).

Therefore, the resultant state conditioned on the outcomes of the noisy BSM is

$$\begin{aligned}\rho_{AB|b=j} &= \sum_{i=1}^{4} P(\psi_i|b=j)\rho_{AB|\psi_i} \\ &= \sum_{i=1}^{4} P(\psi_i|b=j)\frac{\mathbb{1}_A \otimes |\psi_i\rangle\langle\psi_i|\rho_{AB}\mathbb{1}_A \otimes |\psi_i\rangle\langle\psi_i|}{\mathrm{Tr}(\mathbb{1}_A \otimes |\psi_i\rangle\langle\psi_i|\rho_{AB})}.\end{aligned}$$

With this, we can calculate the CHSH violation values of A_1 and A_2 as in the previous section, by taking the expectation value of the Bell operator. For example, the expectation value of the bell operator $\hat{\mathcal{S}}$ defined in Eqn.5.3, given that noisy BSM output $b = 1$, depends on P according to

$$\mathcal{S}(P) = \frac{2\sqrt{2}(P_{11} - P_{41})}{P_{11} + P_{21} + P_{31} + P_{41}}. \tag{5.5}$$

In a perfect BSM, the only non-zero term in the above expression is $P_{11} = 1$, and we recover the optimal violation of $2\sqrt{2}$. One can easily verify that for the case $\rho_{AB} = |\Phi^+\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2}$, the above expression corresponds to

$$\begin{aligned}\mathcal{S}(P) &= 2\sqrt{2}(P(\psi_1|b=1) - P(\psi_4|b=1)) \\ &= \sum_{i=1}^{4}\langle\hat{\mathcal{S}}\rangle_i P(\psi_i|b=1),\end{aligned}$$

where $\langle\hat{\mathcal{S}}\rangle_i$ is the expectation value of $\hat{\mathcal{S}}$ evaluated on the state $|\psi_i\rangle$. This is the expected result since the output $b = 1$ corresponds to a probabilistic mixture of outcomes ψ_i of the original BSM.

5.3 Entangling Measurements

In the previous sections, we have seen how the statistics will change if the state in test (i) and the BSM in test (ii) of the protocol deviates from the ideal case. However, it is important to note that although, for example, when $v = \frac{1}{\sqrt{2}}$ and $\theta = \frac{\pi}{4}$ in section 5.1 will give $\mathcal{S} = \sqrt{2}$, the converse is not true. In other words, we cannot certify that the measurement is a perfect BSM upon seeing $\mathcal{S} = \sqrt{2}$. Indeed, with $v = 1$ and $\theta = 0$, we see the same statistics but Bob's measurement in this case is not a BSM.

However, the criteria of a perfect self-testing result in test (i) together with a maximal CHSH violation in test (ii) seem overly stringent, making certification of non-trivial ququart measurement an impossible task. After all, measurement devices are rarely perfect. Therefore, it will be desirable to relax our criteria. One way to do this is

instead of insisting on a perfect BSM, we may just focus on entangling measurements. A measurement that causes entanglement in initially unentangled systems cannot be achieved by sequential local measurements.

With this relaxed criteria, we can allow for deviations from $\mathcal{S} = 2\sqrt{2}$ in test (ii).

5.3.1 Certifying entangling measurement

It was mentioned in ref. [30] that any deviations from ideal in test (i) will lead to difficulties in certifying entangling measurements, the reason being that we will not be able to conclude that Alice and Bob each holds two subsystems anymore, making the question of whether Bob has performed a entangling measurement inapplicable.

Therefore, we shall restrict ourselves to the case in which the ideal statistics is obtained in test (i). We can thus certify that the state sent to Alice and Bob is, up to local isometry, the state in Eqn. 5.1 with $v = 1$. From Eqn. 5.4, we see that whenever $\theta \neq \frac{k\pi}{2}$, $\mathcal{S} > \sqrt{2}$. In other words, whenever Bob makes a pure entangling measurement, a measurement in which the measurement operators are not separable, the CHSH violation by A_1 and A_2 will always be greater than $\sqrt{2}$. In fact, it turns out that the converse is also true [30]:

Proposition 5.1. $\mathcal{S} > \sqrt{2} \Rightarrow$ *Bob's measurement was entangling.*

Proof. To prove this claim, we have to find the maximum CHSH violation that Alice can obtain given that Bob has made a separable measurement.

From test (i), we know, according theorem 4.1, that

$$\rho_{AB} = (|\Phi^+\rangle\langle\Phi^+|^{\otimes 2})_{A_1B_1A_2B_2} \otimes |junk\rangle\langle junk|_{A'B'}$$

up to local isometries. It follows that if Bob's measurement on the subsystems B_1 and B_2 were not entangling, the resultant partial state $\rho_{A_1A_2|b} = \mathrm{Tr}_{B_1,B_2,A',B'}(\rho_{AB})$ of A_1 and A_2 will be a product state.

Moreover, we also know from self-testing that the four measurements of Alice is equivalent to the observables $\{\hat{Z}, \hat{X}, \frac{\hat{Z}+\hat{X}}{\sqrt{2}}, \frac{\hat{Z}-\hat{X}}{\sqrt{2}}\}_{A_1A_2} \otimes \mathbb{1}_{A'}$ up to local isometries. Hence, any CHSH Bell-operator constructed out of these four measurements must have the form $\beta_{A_1A_2} \otimes \mathbb{1}_{A'}$. In other words, entanglement in A' will not contribute to the CHSH violation observed by Alice. This can be calculated from $\mathrm{Tr}((\beta_{A_1A_2})\rho_{A_1A_2|b})$ where $\beta_{A_1A_2}$ is some operator acting on a 2-qubit Hilbert space and $\rho_{A_1A_2|b}$ is some 2-qubit state.

Therefore, the maximum violation that Alice can observe after a non-entangling measurement by Bob will be given by

$$\mathcal{S}_{sep} = \max_{\phi \in \mathcal{P}} \langle \phi | \hat{\mathcal{S}} | \phi \rangle, \tag{5.6}$$

where $\hat{\mathcal{S}}$ is the 2-qubit Bell operator in Eqn. 5.3 and $|\phi\rangle$ is some 2-qubit state. The maximization is taken over the set of pure product states, $\mathcal{P}$, since the set of separable states is convex and the maximum will be attained over the subset of extremal points, $\mathcal{P}$.

One can easily verify that the spectral decomposition of $\hat{\mathcal{S}}$ is given by $\hat{\mathcal{S}} = 2\sqrt{2}(|\Phi^+\rangle\langle\Phi^+| - |\Phi^-\rangle\langle\Phi^-|)$. Putting this into the above expression, we obtain

$$\begin{aligned} \mathcal{S}_{sep} &= \max_{\phi \in \mathcal{P}} \langle \phi | \hat{\mathcal{S}} | \phi \rangle \\ &= \max_{\phi \in \mathcal{P}} 2\sqrt{2}(|\langle \phi | \Phi^+ \rangle|^2 - |\langle \phi | \Psi^- \rangle|^2). \end{aligned} \tag{5.7}$$

Finally, as the maximum overlap between a product state and a Bell state is $\frac{1}{2}$, $\mathcal{S}_{sep} = \sqrt{2}$. In summary, if Alice observes any violation value $\mathcal{S} > \mathcal{S}_{sep} = \sqrt{2}$, the state $\rho_{A_1 A_2|b}$ measured must be entangled, which can only be the case if Bob has made an entangling measurement. □

5.4 Overview

With the above exercises, we are now in a position to ask the question "How will imperfections in my devices affect the certification of non-trivial ququart measurement?"

For example, we may consider an experimentalist hoping to show off his experiment set up by demonstrating that his measurement is able to preform an entangling measurement. In his lab, he has a quantum source, which can create entangled qubits. However, due to imperfections in the source, the qubits produced will not be in a perfect singlet state but will be mixed with some white noise, ending up in the Werner state, Eqn. 5.1.

In this case, we will make a small departure from the fully device independent scenario by assuming that in every run of the experiment, the experimentalist sees and knows that his source has sent out two pairs of Werner states, with one qubit from each pair sent to Alice and the other to Bob. In other words, he knows that two uncorrelated qubits were being sent to Alice and two to Bob in each run.

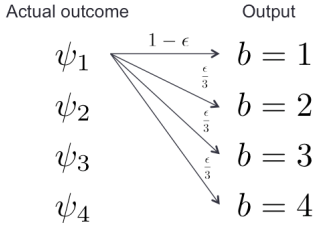


FIGURE 5.1: Noisy measurement. With probability $1-\epsilon$, the device will output the correct b as the outcome of the original measurement, ψ_b. The error ϵ is then distributed evenly amongst the other 3 outputs.

A noisy entangling measurement will then be carried out, which can be parametrised by θ as in Eqn. 5.2, but with mixed outputs, as in section 5.2. For simplicity, we will model the measurement device to output $b = i$ when the original entangling measurement gave the i-th outcome with probability $1-\epsilon$, with ϵ being a small error, which is then equally distributed among the other outputs. This scheme is illustrated in Fig. 5.1.

In such a scenario, we will have three parameters to consider, namely v for the Werner state, θ for the entangling measurement and ϵ for the noisy measurement. We can then perform a calculation similar to that in section 5.2 but replacing the state used in the first step by two pairs of Werner states, and replacing the projectors onto the four Bell states by projectors onto the four orthogonal entangled states in Eqn. 5.2.

As with the previous sections, we will restrict ourselves to looking at the case in which $b = 1$ and the choosing the conventional CHSH operator, $\hat{\mathcal{S}}$ to investigate how the value $\mathcal{S}$ will depend on the three parameters.

After performing the necessary calculations, we find the following dependence

$$\begin{aligned}\mathcal{S}(v,\theta,\epsilon) &= \sum_{i=1}^{4}\langle\hat{\mathcal{S}}\rangle_i P(\psi_i|b=1)\\ &= v^2\sqrt{2}(\sin(2\theta)+1)(1-\frac{4}{3}\epsilon).\end{aligned}$$

As with the noisy BSM case, this result can be intuitively understood as the expectation value of $\mathcal{S}$ since the outcome $b = 1$ is just a probabilistic mixture of the different measurement outcomes, $|\psi_i\rangle$.

In order to certify entangling measurements, we would require $\mathcal{S} > \sqrt{2}$. Fig. 5.2 shows the 3D plot of the three parameters. The region in which (θ, ϵ, v) gives $\mathcal{S} > \sqrt{2}$ is shaded in orange.

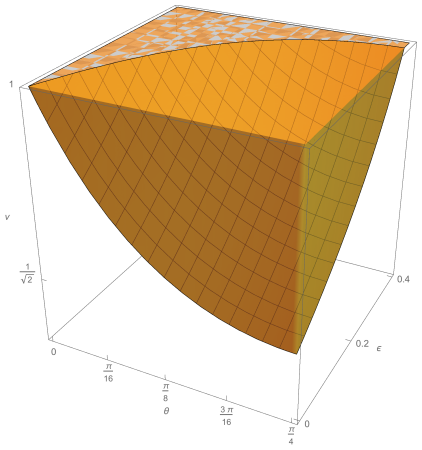
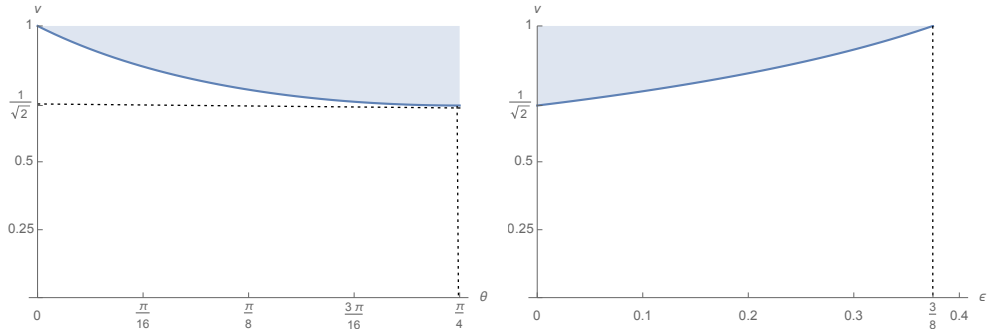


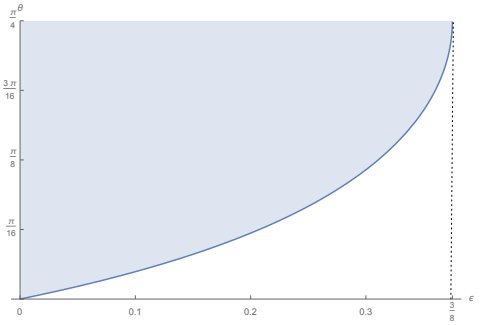
FIGURE 5.2: Region for which (v, θ, ϵ) gives $\mathcal{S} > \sqrt{2}$

The projections of the shaded region onto the $\epsilon = 0$, $\theta = \frac{\pi}{4}$ and $v = 1$ planes are also shown in Fig. 5.3.



(a) Projection onto $\epsilon = 0$

(b) Projection onto $\theta = \frac{\pi}{4}$



(c) Projection onto $v = 1$

FIGURE 5.3: Projections of shaded region. For each of the above figures, only points strictly above the blue curve may be tolerated for certifying entangling measurements.

Each of these figures tells us the amount of imperfections we can tolerate in two of the three parameters, with the last parameter assumed to be ideal. From Figs. 5.3(a) and 5.3(b), we see that in order to certify entangling measurement, the Werner state must

have $v > \frac{1}{\sqrt{2}}$. This is the same limit below which the state stops violating a CHSH test. Therefore, so long as the amount of noise does not exceed what is needed for the Werner state to violate a CHSH test, there will be some combination of (v, θ, ϵ) for which we can still certify entangling measurement.

For the first quadrant, we see that so long as $\theta \neq 0$ or $\frac{\pi}{2}$, we have an entangling measurement which can be certified for some v and ϵ values. Due to the particular $\hat{\mathcal{S}}$ we have chosen to look at, we will not be able to certify entangling measurements when θ lies in the second or fourth quadrant. However, in each quadrant, so long as the measurement is entangling, a suitable s_i in Eqn. 4.4 will result in $\mathcal{S} > \sqrt{2}$.

Finally, the amount of noise beyond which we can no longer certify entangling measurement is $\epsilon < \frac{3}{8}$.

Chapter 6

Conclusion

6.1 Measurements and Unitary Operations

In section 3.1, an alternative motivation for DW was proposed as there was a need to demonstrate genuine access to higher dimensions. We have defined the criteria for this as having the ability to perform all non-trivial measurements on the Hilbert space with the dimension that one is testing. A more natural and suitable criteria would probably be the ability to perform all unitary operations instead of measurements since unitary operations are involved in computation algorithms.

However, certifying measurements may be equivalent to certifying unitary operations if we assume that the measurements are made by first performing unitary transforms which will transform the measurement basis vectors into the computational basis vectors followed by measurements in that basis.

For example, a BSM measurement can be performed by applying a *controlled-NOT*, or CNOT gate on the 2-qubit state, followed by a *Hadamard* gate on the control qubit. Fig. 6.1 shows the corresponding circuit. The effect of the circuit on the four Bell states is given in table 6.1. A measurement on the transformed state in the computational basis is then equivalent to a BSM.

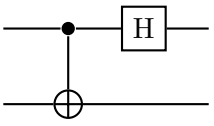


FIGURE 6.1: A quantum circuit for performing a BSM.

The Hadamard gate transforms the $|0\rangle$ state into $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ into $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

In	Out
$\|\Phi^+\rangle$	$\|00\rangle$
$\|\Phi^-\rangle$	$\|10\rangle$
$\|\Psi^+\rangle$	$\|01\rangle$
$\|\Psi^-\rangle$	$\|11\rangle$

TABLE 6.1: The output states for the various inputs to the BSM circuit.

The CNOT gate is a 2-qubit gate, taking one qubit as a *control* and inverting the *target* qubit if the control is in state $|1\rangle$ and leaving the target unchanged otherwise. In other words, the CNOT gate performs the following transformation:

$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle,$$

with the first qubit being the control and the second being the target.

As an explicit example, the CNOT gate takes the input $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ to $\frac{|00\rangle+|10\rangle}{\sqrt{2}}$. The Hadamard gate then takes the control qubit into a superposition: $\frac{(|0\rangle+|1\rangle+|0\rangle-|1\rangle)|0\rangle}{2}$, which thus gives us the state $|00\rangle$.

Therefore, certifying a BSM may be seen as certifying the ability to perform a CNOT gate. If we further assume the ability to perform single qubit unitaries, then we have succeeded in certifying the ability to perform all non-trivial high dimension measurements since CNOT and single qubit gates are *universal* for quantum computation [35]. That is, single qubit and CNOT gates together can be used to implement any arbitrary unitary operations on multiple qubits.

For example, the general entangling measurement in Eqn. 5.2 can be implemented by the circuit in Fig. 6.2. This is a modification of the circuit in Fig. 6.1 by replacing the Hadamard gate with a single qubit unitary which maps $|0\rangle \mapsto \sec(\theta)\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle \mapsto \csc(\theta)\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

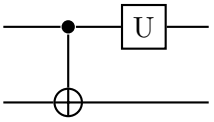


FIGURE 6.2: A quantum circuit for performing a general entangling measurement.

6.2 Further Directions

Any feasible certifications should allow for deviations from ideal and preferably allow some conclusions to be drawn from the observed statistics. Therefore, it will be desirable if the BSM certification proposed in this report can be modified such that one does not need to satisfy test (i) perfectly.

In addition, certifying a BSM constitutes but one possible proper dimension witness. It may be possible that by studying the set of probabilities achievable with factorisable states and measurements, one can find some form of boundaries to this set, much like how the Bell-inequalities are boundaries to the LV polytope. This will make it easier to verify if a given probability point can be achieved using sequential local measurements on low dimensional systems.

Appendix A

Violation of the CGLMP$_3$ DW using sequential qubit measurements

This appendix lists the steps of obtaining the violating points on fig. 3.6 and the relevant matlab codes.

First, we compute the probability table of the qu-8it MES using the optimal measurements:

```
function [p] = Ptable(state)
%compute the probability table of a given state (column) using the "maximum
%violation measurements".

d=sqrt(length(state));

%normalise the state
state0=1/sqrt(state'*state)*state;

% construct the Bell operator (CGLMP operator)
CGLMP = zeros(d^2);

ineq = [triu(ones(d)) tril(ones(d)); tril(ones(d)) -tril(ones(d))];

ineq = reshape(ineq,4*d^2,1);

ii = 1;

for y=0:1
    for b=0:d-1
        for x = 0:1
            for a = 0:d-1
```

```
                CGLMP = CGLMP + ineq(ii)*kron(optimalBasis(d,0,x,a)* ...
                    optimalBasis(d,0,x,a)',optimalBasis(d,1,y,b)* ...
                    optimalBasis(d,1,y,b)');
                ii = ii + 1;

            end
        end
    end
end


p = zeros(4*d^2,1);
ii = 1;
for y=0:1
    for b=0:d-1
        for x = 0:1
            for a = 0:d-1

                p(ii) = state0'*kron(optimalBasis(d,0,x,a)* ...
                    optimalBasis(d,0,x,a)',optimalBasis(d,1,y,b)* ...
                    optimalBasis(d,1,y,b)')*state0;
                ii = ii + 1;
            end
        end
    end
end

p = reshape(p,2*d,2*d);

end
```

Next, we input the probability table as "P" into the function below to obtain the optimal relabeling.

```
function [Index,v] = Optimalrelabel( P )
%to find the index that will result in the maximum violation for the lifted
%CGLMP3 to 8 outcome case
%Take the 8 outcome probability table, P, and compute the best relabel
%for the violation of the CGLMP3 inequality

x = 1:3;                  %// Set of possible letters
K = 8;                       %// Length of each permutation
%// Create all possible permutations (with repetition) of letters stored in x
C = cell(K, 1);              %// Preallocate a cell array
[C{:}] = ndgrid(x);          %// Create K grids of values
y = cellfun(@(x){x(:)}, C); %// Convert grids to column vectors
y = [y{:}];

A=ones(3);
coeffn=[triu(A) tril(A);tril(A) -tril(A)];

Index=[y(1,:) y(1,:)];
v=0;
for i=1:3^8
```

```
    for j=1:3^8
        In=[y(i,:) y(j,:)+3];
        V=sum(sum(coeffn([y(i,:) y(j,:)+3],[y(i,:) y(j,:)+3]).*P));
        if V>v
            v=V;
            Index=In;
        end
    end
end

end
```

Using this relabeling, perform a minimisation using "fminunc" on the function "c8to3vioV2" to obtain a factorisable qu-8it state that will give a higher violation to the CGLMP_3 inequality.

```
function [ c3vio] = c8to3vioV2( x )
%Given the parameters x=(x1 x2... x15) of a factorisable c8*c8 state,
%compute the corresponding cglmp3 violation,assuming the maximum violation
%measurement and using the index
%corresponding to the best lifting
%(3  1  2  3  1  2  3  1  6  4  5  6  4  5  6  4)
%   v=c3vio(x), v=violation. Parametrised state =
%   (cos(x1)|aa'>+sin(x1)|bb'>) * (...)*(...) where
%   |a>=cos(x2)|0>+exp(1i*x3)sin(x2)|1>,
%   |a'>=cos(x4)|0>+exp(1i*x5)sin(x4)|1>

%express the factorisable state in the normal column representation psi,
%with Ai,j being the various |a>s
A10=[cos(x(2)) exp(1i*x(3))*sin(x(2))]'; A11=[sin(x(2)) ...
    -exp(-1i*x(3))*cos(x(2))]';
B10=[cos(x(4)) exp(1i*x(5))*sin(x(4))]'; B11=[sin(x(4)) ...
    -exp(-1i*x(5))*cos(x(4))]';

A20=[cos(x(7)) exp(1i*x(8))*sin(x(7))]'; A21=[sin(x(7)) ...
    -exp(-1i*x(8))*cos(x(7))]';
B20=[cos(x(9)) exp(1i*x(10))*sin(x(9))]'; B21=[sin(x(9)) ...
    -exp(-1i*x(10))*cos(x(9))]';

A30=[cos(x(12)) exp(1i*x(13))*sin(x(12))]'; A31=[sin(x(12)) ...
    -exp(-1i*x(13))*cos(x(12))]';
B30=[cos(x(14)) exp(1i*x(15))*sin(x(14))]'; B31=[sin(x(14)) ...
    -exp(-1i*x(15))*cos(x(14))]';

psi=cos(x(1))*cos(x(6))*cos(x(11))...
    *kron(kron(kron(A10,A20),kron(A30,B10)),kron(B20,B30));
psi=psi+cos(x(1))*cos(x(6))*sin(x(11))...
    *kron(kron(kron(A10,A20),kron(A31,B10)),kron(B20,B31));
psi=psi+cos(x(1))*sin(x(6))*cos(x(11))...
    *kron(kron(kron(A10,A21),kron(A30,B10)),kron(B21,B30));
psi=psi+cos(x(1))*sin(x(6))*sin(x(11))...
    *kron(kron(kron(A10,A21),kron(A31,B10)),kron(B21,B31));
psi=psi+sin(x(1))*cos(x(6))*cos(x(11))...
    *kron(kron(kron(A11,A20),kron(A30,B11)),kron(B20,B30));
```

```
psi=psi+sin(x(1))*cos(x(6))*sin(x(11))...
    *kron(kron(kron(A11,A20),kron(A31,B11)),kron(B20,B31));
psi=psi+sin(x(1))*sin(x(6))*cos(x(11))...
    *kron(kron(kron(A11,A21),kron(A30,B11)),kron(B21,B30));
psi=psi+sin(x(1))*sin(x(6))*sin(x(11))...
    *kron(kron(kron(A11,A21),kron(A31,B11)),kron(B21,B31));

%Obtain the lifted "bell operator", Bell.
state=1/sqrt(psi'*psi)*psi;
Bell3to8;
c3vio=real(state'*Bell*state);




end
```

Using the function "Ptable", we can again compute the probability table corresponding to this state. Next, using the optimal relabeling, we reduce this 8 outcome probability table into the 3 outcome case using

```
function [ Probtable ] = Reddto3PT( Pd,In )
%Given a probability table Pd of d outcomes, find the reduced probability table by
%grouping the outcomes into 3 outcomes using arbitrary indices, In, that is
%symmetric for Alice and Bob and over all measurement settings

d=length(Pd)/2;
%create a function to call on the relabelings

    function [index]= outcome(x)
        if x==1
            index=find(In==1);
        elseif x==2
            index=find(In==2);
        elseif x==3
            index=find(In==3);
        else
            index=0;
        end
    end

Probtable=zeros(6);

for i=1:3
    for j=1:3
        Probtable(i,j)=sum(sum(Pd(outcome(i), outcome(j))));
        Probtable(i+3,j)=sum(sum(Pd(outcome(i)+d, outcome(j))));
        Probtable(i,j+3)=sum(sum(Pd(outcome(i), outcome(j)+d)));
        Probtable(i+3, j+3)=sum(sum(Pd(outcome(i)+d, outcome(j)+d)));
    end
end

end
```

To compute $D(\mathcal{P})$ in Eqn. 3.5, we use:

```
function [ D ] = Dvalue( Prob )
%to find the D(P) given the probability table from a bipartite d outcome
%experiment

d=length(Prob)/2;

P00=Prob(1:d,1:d);
P01=Prob(1:d,(d+1):2*d);
P10=Prob((d+1):2*d,1:d);
P11=Prob((d+1):2*d,(d+1):2*d);

%to find D for each of the x,y measurements
DP00=0;
DP01=0;
DP10=0;
DP11=0;
for k=0:d-1
    DP00=DP00-P00(k+1,mod(k-1-(0-1)*(0-1),d)+1);
    DP01=DP01-P01(k+1,mod(k-1-(0-1)*(1-1),d)+1);
    DP10=DP10-P10(k+1,mod(k-1-(1-1)*(0-1),d)+1);
    DP11=DP11-P11(k+1,mod(k-1-(1-1)*(1-1),d)+1);
end

D=DP00+DP01+DP10+DP11;

end
```

Finally, to obtain more points on the figure, we use this script:

```
%calculate the lifted 3to8 bell operator using the optimal indices
Bell = zeros(64);

cglmp3=[triu(ones(3)) tril(ones(3)); tril(ones(3)) -tril(ones(3))];
index=[3  1  2  3  1  2  3  1  6  4  5  6  4  5  6  4];
liftc3=cglmp3(index, index);

ineq = reshape(liftc3,4*64,1);

ii = 1;

for y=0:1
    for b=0:8-1
        for x = 0:1
            for a = 0:8-1

                Bell = Bell + ineq(ii)*kron(optimalBasis(8,0,x,a)...
                    *optimalBasis(8,0,x,a)',optimalBasis(8,1,y,b)...
                    *optimalBasis(8,1,y,b)');
                ii = ii + 1;

            end
        end
    end
```

```
end

Bell;

%randomly select 50 cp values between 2 and 2.3 made by reducing qu8it
%to qutrit case and give the pair (cp,dp)

x=2+(2.3-2).*rand(1,50);
for i=1:50
    cp=x(i);
    initAngle=rand(1,15);
func =@(w)-abs(c8to3vio(w)'*Bell*c8to3vio(w));
gunc =@(w) (func(w)-(-cp))^2;
[r,rv]=fminunc(gunc,initAngle);
%c1=c8to3vioV2(r) %just for consistency check
P=Ptable(c8to3vio(r));
P3=Reddto3PT(P,[3 1 2 3 1 2 3 1]);
D=Dvalue(P3);
C=sum(sum(cglmp3.*P3));
    y(i)=D;
    x1(i)=C-2;
end
y=real(y)
x=real(x1)
plot(y,x)
```

Appendix B

Deviation from ideal BSM

This appendix includes the matlab codes used for sections 5.1 and 5.2.

The below script is used to obtain the expression in Eqn. 5.4:

```
%2 by 1 unit vectors
e1=[1;0]; e2=[0;1];
%create e to call on dim 16 unit vectors
e=eye(16); %eg., e(:,3)=e3 in dim 16

%create the unitary to change from basis of B=A1B1A2B2 and C=A1A2B1B2
I_CB=[e(1,:);e(2,:);e(5,:);e(6,:);e(3,:);e(4,:);e(7,:);e(8,:);e(9,:);...
      e(10,:);e(13,:);e(14,:);e(11,:);e(12,:);e(15,:);e(16,:)];

%create the four bell states
phi_p = (1/sqrt(2))*(kron(e1,e1)+kron(e2,e2));
phi_m = (1/sqrt(2))*(kron(e1,e1)-kron(e2,e2));
psi_p = (1/sqrt(2))*(kron(e1,e2)+kron(e2,e1));
psi_m = (1/sqrt(2))*(kron(e1,e2)-kron(e2,e1));

%create the starting state werner \otimes werner
v = sym('v','real');
rho_A1B1A2B2=kron(v*(phi_p)*phi_p'+(1-v)/4*eye(4),v*(phi_p)*phi_p'+(1-v)/4*eye(4));
rho_A1A2B1B2=I_CB*(rho_A1B1A2B2)*(I_CB');
rho=rho_A1A2B1B2;

%the projectors projecting Bob's system onto the four (imperfect) bell states
x = sym('x','real'); %x=pi/4 is the perfect bell on Bob
E0=cos(x)*kron(e1,e1)+sin(x)*kron(e2,e2);
E1=sin(x)*kron(e1,e1)-cos(x)*kron(e2,e2);
E2=cos(x)*kron(e1,e2)+sin(x)*kron(e2,e1);
E3=sin(x)*kron(e1,e2)-cos(x)*kron(e2,e1); %operator acts on 2-qubit state

E0=kron(eye(4),E0*(E0'));
E1=kron(eye(4),E1*(E1'));
E2=kron(eye(4),E2*(E2'));
E3=kron(eye(4),E3*(E3'));% operators act on the combined system of Alice and Bob
```

```
%the resultant state of alice and bob conditioned on Bob's measurement
%result
rho_E0=(1/trace(E0*E0'*rho))*(E0*rho*E0');
rho_E1=(1/trace(E1*E1'*rho))*(E1*rho*E1');
rho_E2=(1/trace(E2*E2'*rho))*(E2*rho*E2');
rho_E3=(1/trace(E3*E3'*rho))*(E3*rho*E3');

%sigma x, y, z
sigx=[0 1;1 0]; sigz=[1 0;0 -1];

%the four bell operators
s1=kron(sigz,(1/sqrt(2))*(sigz+sigx))+kron(sigz,(1/sqrt(2))*(sigz-sigx))+...
   kron(sigx,(1/sqrt(2))*(sigz+sigx))-kron(sigx,(1/sqrt(2))*(sigz-sigx));
s2=kron(sigz,(1/sqrt(2))*(sigz+sigx))+kron(sigz,(1/sqrt(2))*(sigz-sigx))-...
   kron(sigx,(1/sqrt(2))*(sigz+sigx))+kron(sigx,(1/sqrt(2))*(sigz-sigx));
s4=-s1; s3=-s2;

%the "optimal" CHSH result of A1 and A2 given the result of Bob
S1=trace(kron(s1,eye(4))*rho_E0);
S2=trace(kron(s2,eye(4))*rho_E1);
S3=trace(kron(s3,eye(4))*rho_E2);
S4=trace(kron(s4,eye(4))*rho_E3);

%test: if v=1 and x=pi/4, S1 to S4 will yield the max vio of 2 sqrt2
v=1;x=pi/4;

%dep on v and x: 2^(1/2)*v^2*(sin(2*x) + 1)
```

The next script is used to obtain the expression in Eqn. 5.5:

```
%To find the CHSH violation of Alice given a noisy BSM on Bob's side where
%the measurement outcomes are mixed up. Mixtures are of the perfect bell
%state measurements, E0-E3, name the outcomes M0-M3.

%2 by 1 unit vectors
e1=[1;0]; e2=[0;1];
%create e to call on dim 16 unit vectors
e=eye(16); %eg., e(:,3)=e3 in dim 16

%create the unitary to change from basis of B=A1B1A2B2 and C=A1A2B1B2
I_CB=[e(1,:);e(2,:);e(5,:);e(6,:);e(3,:);e(4,:);e(7,:);e(8,:);e(9,:);...
      e(10,:);e(13,:);e(14,:);e(11,:);e(12,:);e(15,:);e(16,:)];

%create the four bell states
phi_p = (1/sqrt(2))*(kron(e1,e1)+kron(e2,e2));
phi_m = (1/sqrt(2))*(kron(e1,e1)-kron(e2,e2));
psi_p = (1/sqrt(2))*(kron(e1,e2)+kron(e2,e1));
psi_m = (1/sqrt(2))*(kron(e1,e2)-kron(e2,e1));

%create the starting singlet state
rho_A1B1A2B2=kron((phi_p)*phi_p',(phi_p)*phi_p');
rho_A1A2B1B2=I_CB*(rho_A1B1A2B2)*(I_CB');
rho=rho_A1A2B1B2;

%the projectors on AB projecting Bob's system onto the four bell states
```

```
E0=kron(eye(4),phi_p*(phi_p'));
E1=kron(eye(4),phi_m*(phi_m'));
E2=kron(eye(4),psi_p*(psi_p'));
E3=kron(eye(4),psi_m*(psi_m'));

% create the probabilities for the mixing of Bob's outcome
P=sym('P',[4,3]);
P=[P ones(4,1)-sum(P.').']; %P=['output M0 given E0', 'output M1
%given E0',...;'output M0 given E1'...]

%Probability of getting each of the outcomes
PM0=trace(E0*E0'*rho)*P(1,1)+trace(E1*E1'*rho)*P(2,1)+trace(E2*E2'*rho)...
    *P(3,1)+trace(E3*E3'*rho)*P(4,1);
PM1=trace(E0*E0'*rho)*P(1,2)+trace(E1*E1'*rho)*P(2,2)+trace(E2*E2'*rho)...
    *P(3,2)+trace(E3*E3'*rho)*P(4,2);
PM2=trace(E0*E0'*rho)*P(1,3)+trace(E1*E1'*rho)*P(2,3)+trace(E2*E2'*rho)...
    *P(3,3)+trace(E3*E3'*rho)*P(4,3);
PM3=trace(E0*E0'*rho)*P(1,4)+trace(E1*E1'*rho)*P(2,4)+trace(E2*E2'*rho)...
    *P(3,4)+trace(E3*E3'*rho)*P(4,4);

%the resultant state of alice and bob conditioned on Bob's true measurement
%result
rho_1=(1/trace(E0*E0'*rho))*(E0*rho*E0');
rho_2=(1/trace(E1*E1'*rho))*(E1*rho*E1');
rho_3=(1/trace(E2*E2'*rho))*(E2*rho*E2');
rho_4=(1/trace(E3*E3'*rho))*(E3*rho*E3');

%The resultant state of Alice and Bob upon receiving outcome Mb

rho_M0=(1/PM0)*(trace(E0*E0'*rho)*P(1,1)*rho_1+trace(E1*E1'*rho)*P(2,1)...
    *rho_2+trace(E2*E2'*rho)*P(3,1)*rho_3+trace(E3*E3'*rho)*P(4,1)*rho_4);
rho_M1=(1/PM1)*(trace(E0*E0'*rho)*P(1,2)*rho_1+trace(E1*E1'*rho)*P(2,2)*...
    rho_2+trace(E2*E2'*rho)*P(3,2)*rho_3+trace(E3*E3'*rho)*P(4,2)*rho_4);
rho_M2=(1/PM2)*(trace(E0*E0'*rho)*P(1,3)*rho_1+trace(E1*E1'*rho)*P(2,3)...
    *rho_2+trace(E2*E2'*rho)*P(3,3)*rho_3+trace(E3*E3'*rho)*P(4,3)*rho_4);
rho_M3=(1/PM3)*(trace(E0*E0'*rho)*P(1,4)*rho_1+trace(E1*E1'*rho)*P(2,4)...
    *rho_2+trace(E2*E2'*rho)*P(3,4)*rho_3+trace(E3*E3'*rho)*P(4,4)*rho_4);


%sigma x, z
sigx=[0 1;1 0]; sigz=[1 0;0 -1];

%the four bell operators
S1=kron(sigz,(1/sqrt(2))*(sigz+sigx))+kron(sigz,(1/sqrt(2))*(sigz-sigx))...
    +kron(sigx,(1/sqrt(2))*(sigz+sigx))-kron(sigx,(1/sqrt(2))*(sigz-sigx));
S2=kron(sigz,(1/sqrt(2))*(sigz+sigx))+kron(sigz,(1/sqrt(2))*(sigz-sigx))...
    -kron(sigx,(1/sqrt(2))*(sigz+sigx))+kron(sigx,(1/sqrt(2))*(sigz-sigx));
S4=-S1; S3=-S2;

%Possible CHSH results of A1 and A2 given the result of Bob
S1=trace(kron(S1,eye(4))*rho_M0);
S2=trace(kron(S2,eye(4))*rho_M0);
S3=trace(kron(S3,eye(4))*rho_M0);
S4=trace(kron(S4,eye(4))*rho_M0);
```

```
%largest value among these depends on P. E.g. if the prob of psi_0 given M0
%is highest among psi_i, then S1 will be largest
%S1=(2^(1/2)*(2*P1_1 - 2*P4_1))/(P1_1 + P2_1 + P3_1 + P4_1)
```

Bibliography

[1] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007.

[2] Rodrigo Gallego, Nicolas Brunner, Christopher Hadley, and Antonio Acín. Device-independent tests of classical and quantum dimensions. *Phys. Rev. Lett.*, 105: 230501, 2010.

[3] Nicolas Brunner, Miguel Navascués, and Tamás Vértesi. Dimension witnesses and quantum state discrimination. *Phys. Rev. Lett.*, 110:150501, 2013.

[4] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, 2002.

[5] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75:4337–4341, 1995.

[6] John Stewart Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195–200, 1964.

[7] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of bell's inequalities using time- varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, 1982.

[8] B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[9] Adetunmise C. Dada, Jonathan Leach, Gerald S. Buller, Miles J. Padgett, and Erika Andersson. Experimental high-dimensional two-photon entanglement and violations of generalized bell inequalities. *Nat Phys*, 7(9):677–680, 2011.

[10] Nicolas Brunner, Stefano Pironio, Antonio Acin, Nicolas Gisin, André Allan Méthot, and Valerio Scarani. Testing the dimension of hilbert spaces. *Phys. Rev. Lett.*, 100:210503, 2008.

[11] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[12] Valerio Scarani. The device-independent outlook on quantum physics. *Acta Physica Slovaca*, 62(4):347–409, 2012.

[13] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[14] B.S. Tsirelson. Some results and problems on quantum bell-type inequalities. *Hadronic Journal Supplement*, 8:329–345, 1993.

[15] Tamás Vértesi and Károly F. Pál. Bounding the dimension of bipartite quantum systems. *Phys. Rev. A*, 79:042106, 2009.

[16] Károly F. Pál and Tamás Vértesi. Efficiency of higher-dimensional hilbert spaces for the violation of bell inequalities. *Phys. Rev. A*, 77:042105, 2008.

[17] Stephanie Wehner, Matthias Christandl, and Andrew C. Doherty. Lower bound on the dimension of a quantum system given measured data. *Phys. Rev. A*, 78:062112, 2008.

[18] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88:040404, 2002.

[19] Dagomir Kaszlikowski, L. C. Kwek, Jing-Ling Chen, Marek Żukowski, and C. H. Oh. Clauser-horne inequality for three-state systems. *Phys. Rev. A*, 65:032118, Feb 2002. doi: 10.1103/PhysRevA.65.032118. URL `http://link.aps.org/doi/10.1103/PhysRevA.65.032118`.

[20] Daniel Collins and Nicolas Gisin. A relevant two qubit bell inequality inequivalent to the chsh inequality. *Journal of Physics A: Mathematical and General*, 37(5): 1775, 2004.

[21] Valerio Scarani, Nicolas Gisin, Nicolas Brunner, Lluis Masanes, Sergi Pino, and Antonio Acín. Secrecy extraction from no-signaling correlations. *Phys. Rev. A*, 74: 042339, 2006.

[22] Tobias Moroder, Jean-Daniel Bancal, Yeong-Cherng Liang, Martin Hofmann, and Otfried Gühne. Device-independent entanglement quantification and related applications. *Phys. Rev. Lett.*, 111:030501, 2013.

[23] Cai Yu. Quantum sizes: Complexity, dimension and many-box locality. *PhD thesis*, 2015.

[24] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:032314, 2002.

[25] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM review*, 38(1):49–95, 1996.

[26] A. Acín, T. Durt, N. Gisin, and J. I. Latorre. Quantum nonlocality in two three-level systems. *Phys. Rev. A*, 65:052325, 2002.

[27] Stefan Zohren and Richard D. Gill. Maximal violation of the collins-gisin-linden-massar-popescu inequality for infinite dimensional states. *Phys. Rev. Lett.*, 100: 120406, 2008.

[28] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[29] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "event-ready-detectors" bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, 1993.

[30] Rafael Rabelo, Melvyn Ho, Daniel Cavalcanti, Nicolas Brunner, and Valerio Scarani. Device-independent certification of entangled measurements. *Phys. Rev. Lett.*, 107: 050502, 2011.

[31] M McKague, T H Yang, and V Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[32] Sandu Popescu and Daniel Rohrlich. Which states violate bell's inequality maximally? *Physics Letters A*, 169(6):411 – 414, 1992. ISSN 0375-9601.

[33] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. arxiv:1512.02074 [quant-ph].

[34] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, 2000.

[35] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.