SELF-TESTING:

WALKING ON THE BOUNDARY OF THE QUANTUM SET

XINGYAO WU

(B.SC., UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA)

A THESIS SUBMITTED
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

CENTRE FOR QUANTUM TECHNOLOGIES

NATIONAL UNIVERSITY OF SINGAPORE

SUPERVISOR:
PROFESSOR VALERIO SCARANI

EXAMINERS:
ASSOCIATE PROFESSOR DAGOMIR KASZLIKOWSKI
ASSISTANT PROFESSOR JOSEPH FITZSIMONS

Centre for
Quantum
Technologies

OCTOBER 15, 2016

Declaration

I hereby declare that this thesis is my original work and has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.

Xingyao Wu

October 15, 2016

Publications

Y.-Z. Zhen, K. T. Goh, Y.-L. Zheng, W.-F. Cao, X. Wu, K. Chen and V. Scarani. Non-local games and optimal steering at the boundary of the quantum set, *Phys. Rev. A* **94**, 022116, 2016.

X. Wu, J.-D. Bancal, M. McKague, and V. Scarani. Device-independent parallel self-testing of two singlets, *Phys. Rev. A* **93**, 062121, 2016.

Y. Wang, X. Wu and V. Scarani. All the self-testings of the singlet for two binary measurements, *New J. Phys.*, **18**, 025021, 2015.

X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal and V. Scarani. Robust self-testing of the 3-qubit W state, *Phys. Rev. A* **90**, 042339, 2014.

H. N. Le, Y. Cai, X. Wu, R. Rabelo and V. Scarani. Maximal tree size of few-qubit states, *Phys. Rev. A* **89**, 062333, 2014.

H. N. Le, Y. Cai, X. Wu and V. Scarani. Tree-size complexity of multiqubit states, *Phys. Rev. A* **88**, 012321, 2013.

Acknowledgments

First of all, I would like to thank Prof. Valerio Scarani. Without his constant guidance and help, I would not have finished the project to the point as that of now. Working with him, I learned a lot of things including the proper attitudes and methods that are required to be a qualified scientific researcher. I would also like to thank him for his efforts in creating such a lively and harmonious environment in the group. It helps the members of our group collaborate more easily and efficiently. Moreover, it brings us a lot of happiness in the life beyond science research.

I would also like to thank Jean-Daniel Bancal, who offered a lot of help that makes part of the project possible. It is really a nice experience to work with him. I also learned a lot from the way he views and solves the problems, which I think is quite important for a good scientific researcher.

I would also like to offer my sincere thanks to Yu Cai, with whom I had a lot of discussions during the last four years. It is the discussions with him that makes me get rid of a lot of detours when I was stuck to problems encountered in the research.

Besides, I would like to thank all the colleagues who worked with me in the last few years, including Huy Nguyen Le, Tzyh Haur Yang, Yiming Wang, Colin Teo, Alexandre Roulet, Rafael Rabelo, Melvyn Ho, Phuc Thinh Le, Yun Zhi Law, Stefan Nimmrichter, Juan Miguel Arrazola Mantilla, Dai Jibo, Wan Cong, Ernest Tan, Koon Tong Goh, Angeline Shu Sze Yi, Lana Sheridan, Jiri Minar, Yukun Wang and Yuqian Zhou. Without you, my Ph.D. life will not be as enjoyable as what I have now.

Next, I would like to thank my collaborators Matthew McKague, Yi-Zheng Zhen, Yu-Lin Zheng, Wenfei Cao and Kai Chen for sharing their scientific ideas with me that make a lot of research possible.

Most importantly, I would like to thank all my families and my friends for their support and caring about me.

Lastly, I would like to thank both Centre for Quantum Technologies and National University of Singapore which give me the opportunity to study here as a Ph.D. student.

Contents

Chapter 1

Bell nonlocality

Quantum mechanics was born with a lot of counter-intuitive phenomena. Among those, Bell nonlocality is one of the popular topics that has been studied intensively recent years. In this chapter, we will introduce some basic notions and background knowledge about nonlocality which are already known before. This will be helpful for the main study on self-testing in later chapters.

1.1 Bell inequality

Suppose two players named Alice and Bob are playing a game against Eve. Alice and Bob both have a box (or machine) at their sites. Each box has two buttons and two lights on it, while one of the buttons being pressed will consequently lead one of the lights to be switched on (of course, it is not fixed which light will be switched on each time). Without loss of generality, we label the different buttons of Alice and Bob as $(x, y) \in \{0, 1\}$, and the different lights of Alice and Bob as $(a, b) \in \{0, 1\}$. Eve will give the order of which buttons Alice and Bob should press for each run. Then Alice and Bob will operate on their sites and submit the results of a and b to Eve. Eve will calculate $a \oplus b$. Alice and Bob win if $a \oplus b = xy$ (modulo 2) or lose otherwise. We can list the truth table for clarity as in Table 1.1.

For a given measurement setting (x, y), the winning probability for Alice and Bob is

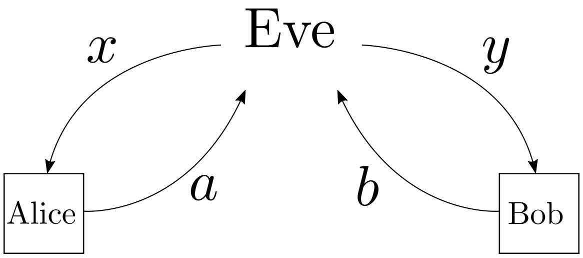


Figure 1.1: The XOR game.

x	y	a	b	x	y	a	b
0	0	0	0	0	1	0	0
		1	1			1	1
1	0	0	0	1	1	0	1
		1	1			1	0

Table 1.1: List of cases when Alice and Bob will win.

$$\mathcal{P}_{xy} = \begin{cases} p(a = b = 0) + p(a = b = 1), & xy = 0, \\ p(a = 0, b = 1) + p(a = 1, b = 0), & xy = 1. \end{cases} \tag{1.1}$$

where p is the probability of the event. It could also be expressed in a simpler way as

$$\mathcal{P}_{xy} = \frac{1 + (-1)^{xy} E_{xy}}{2}, \tag{1.2}$$

where E_{xy} is defined as the *correlation coefficient* $\sum_{a,b} p(a = b|x, y) - p(a \neq b|x, y)$.

This game can also be cast in another way. Suppose Alice and Bob (we will call them A and B instead for convenience) both have one black box (by which we mean they know nothing about the box itself) at their sites. Each box has two measurement settings labeled as $x \in \{0, 1\}$ for A and $y \in \{0, 1\}$ for B. With unbiased choice of measurement settings (x, y), the two black boxes will produce two outcomes (a, b).

The purpose of the game is to maximize the following function of probabilities

$$\mathcal{B} = E_{00} + E_{01} + E_{10} - E_{11}, \tag{1.3}$$

where E_{xy} is defined as in (1.2). It can be shown [1] that with any classical strategy without A and B communicating, the maximum value of $\mathcal{B}$ is 2

$$\mathcal{B} \leq 2. \tag{1.4}$$

However, in the case that Alice and Bob are able to use quantum resources, for instance a maximally entangled state of two qubits, the inequality is able to be violated maximally to $2\sqrt{2}$ [2]. Such a game is normally called a Bell test and the above inequality is well known as the Clauser-Horne-Shimony-Holt (CHSH) inequality [1]. With its original form given by John Bell [3], a reply to the Einstein-Podolsky-Rosen (EPR) paradox [4], the CHSH inequality imposes a non-trivial constraints on the statistics given by the Bell test.

1.2 Correlations

The correlations arising from the game described in the previous section in fact can be divided into several different categories depending on the constraints that are applied to the system. To continue the discussion, we first introduce the formal mathematical description of the game.

Suppose Alice and Bob each have a system which they can perform measurements. Each of them can have m different choices of measurements and each measurement will have n possible outputs. We remove the limitation for the numbers of the measurement choices and the outputs to be binary here to make it more general. We label the inputs of Alice and Bob for the measurements they choose as x, $y \in \{0, 1, ..., m\}$ and the outputs as a, $b \in \{0, 1, ..., n\}$. Such a measurement setting is always called $(2, m, n)$ scenario, where 2 means two parties, m stands for the number of choice of measurements for each party and n stand for the number of the outputs for each measurements, for instance, the game described in the previous section is the (2,2,2) scenario. For the pair of input (x, y), we use $p(ab|xy)$ to denote the probability that output pair (a, b) occurs.

It is easy to see that for given input (x, y), the normalization condition and positivity constraint apply

$$\sum_{a,b} p(ab|xy) = 1 \tag{1.5}$$

$$p(ab|xy) \geq 0 \tag{1.6}$$

Except for the basic constraints (1.5-1.6), depending on different extra constraints, the probability distribution $p(ab|xy)$ has three main types. These three types of categories turn out to be in different hierarchic levels. We will introduce in a descending order regarding the size of the set.

1.2.1 No-signalling correlations

As we have already mentioned in the previous section, a natural constraint that we can impose on the game is that A and B is not allowed to communicate between each other. This is essential to make the game non-trivial, since with communication A and B could output whatever values that are required to win the game according to certain rules. It is not difficult to see that A and B could have a pre-established agreement and once any of A and B broadcasts his or her input, the other one could choose which output he or she needs to produce. With such tricks, the value of (1.3) could be easily reached to 4.

To sum up the idea of no-signalling [2, 5], it basically says that before any of A and B produces his or her output of the measurement, he or she cannot know the inputs of other one. If we write this requirement down as mathematical equations, it is simply

$$\sum_b p(ab|xy) = \sum_b p(ab|xy') \qquad \text{for any } a,\ x,\ y \text{ and } y', \tag{1.7}$$

$$\sum_a p(ab|xy) = \sum_a p(ab|x'y) \qquad \text{for any } b,\ y,\ x \text{ and } x'. \tag{1.8}$$

These equations tell that, no matter what input A gets, from the observation B, he cannot tell which measurement A has made, and the other way around. This avoids the possibility that A and B can use the probability patterns to signal between each other. Hence, if equations (1.7-1.8) are guaranteed, the signalling of the measurement settings (x, y) could be precluded.

A typical type of no-signalling correlation is the PR-box correlation discovered by Popescu and Rohrlich in 1994 [5]. The joint probability is given by

$$p(ab|xy) = \begin{cases} \frac{1}{2}, & \text{if } a \oplus b = xy, \\ 0, & \text{otherwise.} \end{cases} \tag{1.9}$$

Up to now, there is no evidence of the existence of the PR-box correlation in nature and it is not clear whether such correlation exists or not, however, it is beyond the discussion of this thesis.

1.2.2 Quantum correlations

As suggested by the name, quantum correlations are the ones that could be achieved using quantum systems. In this case, the two boxes at A and B could be parts of any quantum state, and the measurements performed on them could also be any measurements on their quantum sub-systems. In order to keep the non-triviality, we inherit the no-signalling constraint. In this sense, we could infer easily that the set of no-signalling correlations is larger than or at least equal to the set of quantum correlations. Under the principle of quantum mechanics, the statistics given by such a game could be expressed as

$$p(ab|xy) = \mathrm{Tr}(\rho_{AB} M_{a|x} \otimes N_{b|y}), \tag{1.10}$$

where ρ_{AB} is the state of the quantum system, $M_{a|x}$ and $N_{b|y}$ are the elements of the corresponding measurements on A and B given inputs x and y respectively. Normally, these measurements could be represented as positive operator-valued measure (POVM) [6]. We write the measurements as a tensor product form since the way the game is played does not allow non-local measurements. A and B performs their measurements separately and measurements are absolutely commuting with each other.

1.2.3 Classical correlations

Classical correlations represent the set of correlations that could be achieved by classical systems, also called local correlations. Again we inherit the no-signalling constraint for non-triviality. In the classical world, there is no superposition as in quantum physics. Determinism, which plays an important role in classical physics, suggests that the outputs of A and B are both determined as soon as the inputs are chosen.

The simplest classical correlations are the deterministic correlations, which means whenever an input is chosen on one side of A and B, the output of him or her will be determined. Formally, it will be

$$p_d(ab|xy) = \begin{cases} 1, & \text{if } a = a_x \text{ and } b = b_y, \\ 0, & \text{otherwise.} \end{cases} \tag{1.11}$$

However, from the perspective of $p(ab|xy)$, there could be uncertainty in the process, and these uncertainties could be possessed by A and B, or even the box itself. This is not against the determinism of classical mechanics but just a matter that we do not have enough knowledge about the system itself. Normally, we associate these knowledges that we have no information as the *local hidden variable* denoted by λ [3].

Sometimes, the λ is also called *shared randomness* between A and B, whether it is between A and B or the boxes.

With the introduction of the local hidden variable λ, the local probability distribution for a classical model will take the form of $p(a|x,\lambda)$ and $p(b|y,\lambda)$. The input of one side does not appear in the output of another side is due to the no-signalling assumption. One may argue that the $p(a|x,\lambda)$ and $p(b|y,\lambda)$ here could also be random, say $p(a|x,\lambda) = p(a|x,\lambda,\lambda')$ and $p(b|y,\lambda) = p(b|y,\lambda,\lambda')$. However, it could be proved that λ' could be absorbed with λ into one local hidden variable [7, 8]. Hence, it is sufficient to consider only the deterministic local hidden variable model $p_d(a|x,\lambda)$ and $p_d(b|y,\lambda)$.

Now we can write the joint probability as

$$p(ab|xy) = \int_\lambda d\lambda \rho(\lambda) p_d(a|x,\lambda) p_d(b|y,\lambda), \tag{1.12}$$

where $\rho(\lambda)$ is the probability density function of λ and $\int_\lambda \rho(\lambda) d\lambda = 1$. One thing should be noticed here is that, we have already assumed that the distribution of the local hidden variable is not affected by the input x and y, this is usually called *measurement independence* condition. We do not consider this situation since it is normally treated as a separate topic as one can never verify where an experiment is measurement independent or not. Moreover, once measurement independence is violated, the no-signalling assumption could also be violated. As shown in [9], it could be proved that any classical correlation could be rewrote into the formalism (1.12). This is important since it infers that the set of classical correlation is actually convex and any point in this set could be expressed as a convex combination of the deterministic points (1.11).

1.3 Two polytopes and the quantum set

As we have discussed in section 1.2, the correlations that correspond to the bipartite game could be divided into different categories by assuming different constraints. The more constraints we impose on the system, the smaller the size of the correlation set will be. It is not difficult to see that the no-signalling set is the largest one and the classical set (also called the local set) is the smallest one. The purpose of this section is to discuss a little bit more about properties and relations of these different sets, specially how to characterize them properly. We will see that the no-signalling and local set could actually be characterized with polytopes in the probability space and the quantum set could be characterized by the Navascués-Pironio-Acín (NPA) hierarchy [10, 11].

1.3.1 The polytope and facets

In fact, for a certain game, we could denote the statistics with a point in the space spanned by $p(ab|xy)$, denoted as $\mathcal{P}$. The dimension of the subspace that p lives could be easily derived as $m^2n^2 - m^2$, where the minus sign is due to the normalization constraints (1.5).

The set of no-signalling correlations is normally denoted by $\mathcal{NS}$. It has the least constraints applied to the behaviour of the probability distributions. The dimension of the $\mathcal{NS}$ set in the $\mathcal{P}$ space could be easily calculated.

$$\mathrm{dim}\mathcal{NS} = m^2n^2 - m^2 - 2(m^2 - m)n + 2m(m-1), \tag{1.13}$$

where the third term is due to the no-signalling constraints (1.7-1.8) and the forth term is due to the fact that there are actually redundant equations if one combines the normalization constraints and part of the no-signalling constraints. Since all the constraints for the set of $\mathcal{NS}$ are linear, it is not difficult to see that the region that represents the set in the space $\mathcal{P}$ is a polytope. With the same reason, the set of local correlations, denoted by $\mathcal{L}$, could also be found as a polytope in the space $\mathcal{P}$.

If we take a look at the constraints that are associated with the set of quantum correlation, denoted by $\mathcal{Q}$, and the set of local correlations $\mathcal{L}$,, they actually do not decrease the number of the free variables. Hence, the dimensions of the set $\mathcal{Q}$ and $\mathcal{L}$ are the same as the dimension of the set of $\mathcal{NS}$, which is equal to (1.13). In a short summary, the sets of $\mathcal{NS}$, $\mathcal{Q}$ and $\mathcal{L}$ all live in the space of $\mathcal{P}$ with the same dimension, and it is easy to see that $\mathcal{L} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$.

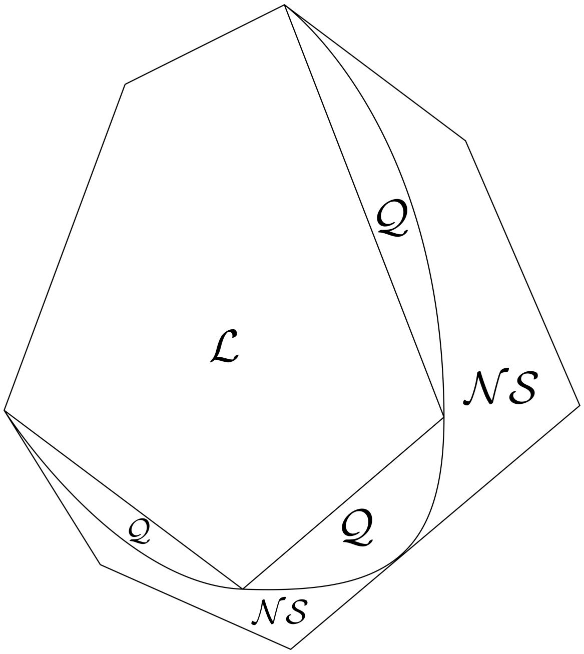


Figure 1.2: A sketch that shows the relation of the no-signalling set $\mathcal{NS}$, the quantum set $\mathcal{Q}$ and the local set $\mathcal{L}$. They are all convex, besides, the sets $\mathcal{NS}$ and $\mathcal{L}$ are described by polytopes.

One of the interesting topics to study about these different sets is the boundary properties. For the local set $\mathcal{L}$ and the no-signalling $\mathcal{NS}$, they are the facets of the polytopes and they are flat. Therefore, the remaining question is to find out these facets. Especially a detailed characterization of the boundary of the local set will give us the ability to differentiate classical behaviours and quantum behaviours.

As we have discussed in the previous section, all classical correlations could be explained as convex combinations of the deterministic points (1.11), then, these deterministic points forms the extremal points of the polytope of $\mathcal{L}$. To characterize the facets, we use the outward-pointing normal vector $\boldsymbol{n}$. It is not a bad idea to choose fully mixed point O as the reference point. Therefore, the inequality corresponding to a facet of $\mathcal{L}$ could be expressed as

$$\boldsymbol{n} \cdot \overrightarrow{OP} \leq s, \tag{1.14}$$

where $\overrightarrow{OP}$ is the vector pointing from O to the point P representing an arbitrary point in the space of $\mathcal{P}$, and s is a constant that could be determined later. The equal sign takes place when P is on the facet. If we expand the vectors in the form of its coordinates, it will become

$$\sum_{abxy} n_{xy}^{ab} p(ab|xy) \leq s \tag{1.15}$$

for the points that are in $\mathcal{L}$. The inequality above is normally called a Bell inequality.

For the case of $m = 2$ and $n = 2$, the local polytope and its facets are completely solved by Froissard [12] and later by Fine [7] independently. It of course includes the inequality (1.4) as shown in section 1.1. Moreover, it is shown that the CHSH inequality with its variants when relabelling the inputs and outputs are the only facets of this scenario [13].

For the cases of m and n not equal to 2, the Bell inequalities are also well studied, for instance, when $m = 2$ and n is arbitrary, the Collins-Gisin-Linden-Massar-Popescue (CGLMP) inequality [14, 15] gives,

$$[a_1 - b_1] + [b_1 - a_2] + [a_2 - b_2] + [b_2 - a_1 - 1] \geq d - 1, \tag{1.16}$$

where $[a_x - b_y] = \sum_{k=0}^{n-1} kp(a_x - b_y = k \mod n)$ and $n = d$ is number of outputs of each subsystem. It could be verified that this inequality reduces to the CHSH inequality (1.4) when $n = 2$.

For the case of both m and n to be arbitrary, the CGLMP inequality was extend to

$$[a_1 - b_1] + [b_1 - a_2] + [a_2 - b_2] + ... + [a_m - b_m] + [b_m - a_1 - 1] \geq d - 1, \tag{1.17}$$

by Barrett et el. [16].

Bell inequalities play an important role in the study of the relation between quantum and classical correlations. It is a very straight forward benchmark that tells the difference of these two behaviours. A violation of a Bell inequality will definitely suggest that the system involved displays non-local properties to some extend. This is often used as a tool to detect entanglement of quantum resources [17, 18, 19]. They are also often used in the experiments as well, such as the famous Bell test experiments [20, 21, 22, 23], loophole free test [24, 25, 26], random number generation [27, 28], etc.

In general, the inequalities from the facets could be derived systematically with the aid of computer programs, for instance PORTA [29]. However, the complexity of the problem grows very fast as the number of the inputs and outputs of the game increase.

1.3.2 The quantum set and NPA hierarchy

Like the no-signalling and local set, quantum set is also convex due to the fact that any mixture of points in the quantum set could always be realized by quantum mechanics. However, it is not true that the $\mathcal{Q}$ is still a polytope in the probability space. Therefore, the boundary of $\mathcal{Q}$ is generally not flat and not as easy as $\mathcal{L}$ to be characterized .

A lot of efforts have been dedicated to characterize the quantum set $\mathcal{Q}$, such as information causality [30]. In this thesis, we will concentrate more on the NPA criterion, which was first introduced by Navascués et. al. in 2008 [10, 11]. It is a criterion that asymptotically approaches the quantum set. Later in 2012, it was used for self-testing and this also brings new perspectives to self-testing itself [31, 32]. We will first discuss the NPA characterization of quantum set in this section and later in the next chapter discuss the application to self-testing.

To begin with, we will first introduce the idea of a sequence of operators. For the two party game as we described above, without knowing the dimension of the system, we will see later in the next chapter that it is always reasonable to assume the measurements to be projective and the state of the system is in a pure state $|\phi\rangle$. A sequence S is a set of operators which are monomial products of the measurement projectors $\Pi_{a|x}$ and $\Pi_{b|y}$, defined as

$$S = \{\mathbb{1}\} \cup \{\Pi_{a|x}\} \cup \{\Pi_{b|y}\} \cup \{\Pi_{a|x}\Pi_{a'|x'}\} \cup \{\Pi_{b|y}\Pi_{b'|y'}\} \cup \{\Pi_{a|x}\Pi_{b|y}\}.... \tag{1.18}$$

The elements goes from identity to the products of infinite number of projectors. However, if we choose to cut at some place, for instance, products of up to n projectors, then we can define a sequence of level n

$$\begin{aligned} S_n = \{\mathbb{1}\} \cup \{\Pi_{a|x}\} \cup \{\Pi_{b|y}\} \cup \{\Pi_{a|x}\Pi_{a'|x'}\} \cup \{\Pi_{b|y}\Pi_{b'|y'}\} \cup \{\Pi_{a|x}\Pi_{b|y}\}... \\ ... \cup \{\underbrace{\Pi_{a|x}\Pi_{a'|x'}...\Pi_{b|y}\Pi_{b'|y'}...}_{n \text{ projectors}}\}. \end{aligned} \tag{1.19}$$

It is not difficult to see that $S_0 = \{\mathbb{1}\}$. Now we can bring up the first NPA result.

Proposition 1. *Suppose a probability distribution p could be explained by quantum physics. If a group of operators $\mathcal{O} = \{O_i\}_{i=1}^n$ satisfies*

$$\sum_{i,j} a_{ij}^k \langle\phi| O_i^\dagger O_j |\phi\rangle = f_k(p), \qquad k = 1, ..., m, \tag{1.20}$$

where a_{ij}^k are real coefficients, $|\phi\rangle$ represents the state of the system and f_k are linear functions of the probabilities $p(ab|xy)$, then, there must exist a $n \times n$ positive semidefinite matrix Γ such that

$$\Gamma \geq 0, \tag{1.21}$$

where Γ is called a certificate.

Proof. It is reasonable to define $\Gamma = \langle\phi| O_i^\dagger O_j |\phi\rangle$. For any vector $v \in \mathbb{C}^n$,

$$\begin{aligned} v^\dagger \Gamma v = \sum_{i,j} v_i^\dagger \Gamma_{ij} v_j = \sum_{i,j} v_i^\dagger \langle\phi| O_i^\dagger O_j |\phi\rangle v_j = \langle\phi| (\sum_i v_i^\dagger O_i^\dagger)(\sum_j O_j v_i) |\phi\rangle \\ = \langle\phi| V^\dagger V |\phi\rangle \geq 0, \end{aligned} \tag{1.22}$$

where $V = \sum_i O_i v_i$. □

This is a necessary condition for a behaviour p to be quantum. It is not yet a characterization of the quantum set. However, we could think (1.21) as a relaxation of the quantum set. With some certain *certificate* Γ which has finite dimension, it is for sure that the set defined by it will be at least bigger than the quantum set. Having this notion, we could now introduce the hierarchical characterization of the quantum set.

For a behavior p arising from the black box scenario that could be explained by quantum physics, it is reasonable to assume the measurements to be projective and the state of the system to be a pure state. This is due to the fact that we can always increase the dimension of the system studied to include all the necessary physical parts to make the state pure and the measurements projective. Hence, any operator O_i associated with the system could be expressed as a linear combination of the elements belongs to the sequence S_∞. Normally, one cannot include all the elements of S_∞ into any practically solvable problem. We can define a *certificate of order* n as the following.

Definition 1. *A certificate Γ^n is said to be of order n if Γ^n is a $|S_n| \times |S_n|$ matrix and $\Gamma^n_{u,v} = \langle\phi| U^\dagger V |\phi\rangle$, where u, v are the indexes for $U, V \in S_n$.*

If a behavior p allows a *certificate* Γ^n, we say that p belongs to $\mathcal{Q}_n$. Due to the simple fact that the positivity of a matrix always leads to the positivity of its submatrices but not the reverse way, the certificate corresponding to a submatrix will always be a necessary condition for the certificate of the original matrix. From the definition of S_n in (1.19), we know that $S_1 \subseteq S_2 \subseteq S_3 \subseteq ... \subseteq S_n \subseteq ....$ With the reason explained before, it then follows that $\mathcal{Q}_1 \subseteq \mathcal{Q}_2 \subseteq \mathcal{Q}_2 \subseteq ... \subseteq \mathcal{Q}_n \subseteq ....$ As the hierarchy level increase, the set defined by Γ^n will become smaller. To see how well the $\mathcal{Q}_n$ approaches to the quantum set $\mathcal{Q}$[1], we have the following results.

Theorem 1. *If a behavior p allows the certificate for any $n \geq 1$, then p belongs to*

[1] One should know that the quantum set defined here is actually different than the quantum set in (1.10). This is because, in the NPA's work, the commutation rule is defined as $[M_{a|x}, N_{b|y}] = 0$ other than that in (1.10). The former is obviously stricter than the latter one. Thus, this will not affect its application for our purpose, since later we will see, we always try to get a relaxed version of the quantum set when we are using NPA with self-testing.

$\mathcal{Q}$.

We will not give the proof here, one could refer to [11] for details. Basically, a *certificate* $\lim_{n\to\infty}\Gamma^n$ will give the characterization of any quantum behavior. There exist some cases that Γ^n for all $n \geq n_0$ are equivalent, however it is not generally guaranteed. We could see that to fully characterize the quantum set, it requires extremely huge computational power [33], in some cases even impossible [34]. Hence, later we will see what we normally do is to have a relaxed version of Γ^∞, which means some certain Γ^n. This will make a lot problems solvable numerically. In the next chapter, we will also use these results to the main problem we are going to discuss here in this thesis, which is self-testing.

Chapter 2

Self-testing and semidefinite programming

Quantum physics, since last century, has been one of the most successful theory in history. It is also the only theory up to now that could explain phenomena at atomic level. It also has a wide range of applications in modern technologies, like semiconductor, laser, atomic clock, magnetic resonance imaging and so on. Recent years, especially the last two decades, a lot of efforts has been dedicated to bring quantum physics into the field of information science, for instance, there is quantum cryptography that claims to be more secure than classical cryptography [35, 36, 37, 38, 39, 40], there are even experiments that are trying to deploy quantum key distribution between different places with satellites [41]. There are also prototypes of quantum computers that claim to be exponentially faster than classical computers [42]. Hopefully, we are going to do a lot with quantum devices in the future.

Since all quantum devices will inevitably play with quantum states and measurements, it becomes a crucial issue for us to know what is the quantum state in the device and how to manipulate it. However, it is unlikely that people, for instance the customers, will build all these devices from scratch by themselves, like nowadays, nobody will build a computer from resistors and capacitors. They will probably buy these so called quantum devices from some companies. The problem then comes that whether these devices can really produce the quantum state and measurements that are claimed to be there. It is unlikely that we could always open the device and check every elements inside. Even though we could really open the device, it is still not easy for us to know whether certain elements in the devices are the one that play the role or not. This is why people start to think about device independent self-testing.

Self-testing is a device independent way to assess the system and the measurement. In fact, there are also a lot of works which study the properties of the state of the system and the measurements in a device independent manner, for instance, entanglement witness [19], dimension witness [43], measurement overlapping [44] and etc. However, self-testing aims specifically to certify the exact state of the system and the measurements. Unlike tomography, it requires no information about the dimension of the Hilbert space or the inner mechanism of the devices. The only thing required is the statistics from the experiments. Under this scenario, the device of each party in the game could be considered as a black box with buttons and bulbs on it, that the experimentalists can only press the button and check out the on and off of the bulbs. Due to the merit of not requiring the details about the devices, self-testing is used in many interesting problems, for instance, interactive proofs for quantum computation [45, 46], arbitrary randomness amplification [47, 48] and etc.

The story of self-testing goes back to 1992 [49][1], when Popescu and Rohrlich proved a surprising result that if a two party binary game, as we described in the previous chapter, could violate the Bell inequality (1.4) to its maximal quantum value $2\sqrt{2}$, the system that is used in the game must be equivalent to the two-qubit singlet state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ up, which is also call a EPR state, and the measurements on each side are complementary. Here, by singlet state, we mean all the four Bell states since they are equivalent up to local unitaries. In 1998, Mayers and Yao [51] first came up with the term ”self-testing” while they proposed another criterion. The proof of Mayers and Yao was simplified and made robust to small fluctuations by McKague et al. in 2012 [52]. Besides these, a lot more efforts have been dedicated to self-testing in recent years and the zoo of the states that could be self-tested has been enlarged tremendously: self-testing of all multi-partite graph

[1] In fact, in the work of Summers and Werner [50], similar result has also been derived.

state [53]; any pure bipartite entangled state [54]; tripartite non-graph state [55, 56]; one relevant two-qutrit state [32]; all the self-testings of singlet state [57]. One of the main issues of self-testing is that a useful self-testing will give us a robust tolerance to experimental fluctuations. A lot of the works we have mentioned not only give a way to self-test those states in the ideal case, but also provide robustness bounds which are doable regarding current experimental precisions. The robustness bound is normally derived either by analytical ways or numerical methods, which we will talk about a bit later. Recently, a nearly optimal robustness bound was given using a new technique with the help of extraction channels and operator inequalities [58], which give inspirations for finding new ways of deriving the robustness bound.

2.1 Self-testing and its definition

Suppose a vendor comes to you and tries to sell you a so-called quantum device, for instance, a EPR resource. Without opening the device, how could we certify that whether the device could really produce EPR state and we are able to manipulate each part of the EPR pair? This is why the idea of self-testing comes out which aims to assess these devices in both the aspect of the state of the device and the measurements. In this scenario, the devices could be thought as black boxes. The assessment is done device-independently, where by ”device-independent” we mean that we are not assuming the dimension of the Hilbert space or how the devices work inside the boxes. What we are using is only the experimental statistics.

For simplicity, we will first give the formal definition of self-testing for the bipartite case:

Definition 2. *For a bipartite experiment, the probability distribution is given by $p(ab|ij)$, where a, b denote the ath, bth outcome of the ith, jth measurement A_i, B_j locally on A and B, then, p self-tests a quantum state $|\tilde{\phi}\rangle$ and measurements σ_i, σ_j, if there exists a local isometry $\Psi = \Psi_A \otimes \Psi_B$, such that for the state of the device*

$|\phi\rangle$ and the measurements A_i, B_j:

$$\Psi(|\phi\rangle_{\mathcal{AB}} \otimes |\xi\rangle_{\mathcal{A'B'}}) = |junk\rangle_{\mathcal{AB}} \otimes |\tilde{\phi}\rangle_{\mathcal{A'B'}} , \tag{2.1}$$

$$\Psi(A_i B_j |\phi\rangle_{\mathcal{AB}} \otimes |\xi\rangle_{\mathcal{A'B'}}) = |junk\rangle_{\mathcal{AB}} \otimes (\sigma_i \otimes \sigma_j) |\tilde{\phi}\rangle_{\mathcal{A'B'}} , \tag{2.2}$$

where $|\xi\rangle$ is the trusted ancilla qubits which could be taken as $|00\rangle$ normally for convenience.

To be concrete, we are going to see what self-testing is more practically by reviewing the Mayers-Yao test [59] for a maximally entangled state. In this test, each run A will choose to make one dichotomic measurement out of three, and B will choose one dichotomic measurement out of two. A and B are not allowed to communicate which measurement they chose before they perform the measurements. Let us denote the inputs of A and B by $x \in \{0, 1, 2\}$ and $y \in \{0, 1\}$, and the outputs by $a \in \{0, 1\}$ and $b \in \{0, 1\}$. Again, the correlation coefficient is defined as $E_{xy} = \sum_{a,b} p(a = b|x, y) - p(a \neq b|x, y)$, where p is the probability distribution of the measurement results. What the Mayers-Yao test says is that, if quantum physics can explain the process, then the following theorem holds:

Theorem 2. *If the correlations of test satisfy the following relation:*

$$\begin{aligned} E_{00} &= 1, & E_{11} &= 1, \\ E_{01} &= 0, & E_{10} &= 0, \\ E_{20} &= \frac{1}{\sqrt{2}}, & E_{21} &= \frac{1}{\sqrt{2}}, \end{aligned} \tag{2.3}$$

then there exists a local isometry $\Psi = \Psi_A \otimes \Psi_B$, such that for the state of the device $|\phi\rangle$ and the measurements A_i, B_j:

$$\Psi(|\phi\rangle_{\mathcal{AB}} \otimes |\xi\rangle_{\mathcal{A'B'}}) = |junk\rangle_{\mathcal{AB}} \otimes |\Phi^+\rangle_{\mathcal{A'B'}} , \tag{2.4}$$

$$\Psi(A_i B_j |\phi\rangle_{\mathcal{AB}} \otimes |\xi\rangle_{\mathcal{A'B'}}) = |junk\rangle_{\mathcal{AB}} \otimes (\sigma_i \otimes \sigma_j) |\Phi^+\rangle_{\mathcal{A'B'}} , \tag{2.5}$$

where σ-s are the Pauli operations on the ancillary qubits. Since we are free to choose *which state to be the product state ancilla, for convenience, we take* $|\xi\rangle = |00\rangle$.

Proof. In the scenario of device-independent self-testing, we do not assume the dimension of the Hilbert space. Hence, it is reasonable to assume that the measurements A_i and B_j acting on A and B are both projective, and the state of the system is in a pure state $|\phi\rangle$. If we denote the projectors of A_i and B_j as $\Pi_{a|x=i}$ and $\Pi_{b|y=j}$, then

$$\begin{aligned} A_i &= \Pi_{a=0|x=i} - \Pi_{a=1|x=i}, \\ B_j &= \Pi_{b=0|y=j} - \Pi_{b=1|y=j}, \end{aligned} \tag{2.6}$$

moreover,

$$A_i^2 = B_j^2 = \mathbb{1}, \tag{2.7}$$

$$[A_i, B_j] = 0. \tag{2.8}$$

The commutation relation of A_i and B_j is due to the fact that A and B are both applying local measurements and the order of how they apply them should not affect the results. One property that we may use later is that, if two normalized state vectors $|\phi_1\rangle$ and $|\phi_2\rangle$ satisfy $\langle\phi_1|\phi_2\rangle = \cos\theta$, then we can conclude that the angle formed by the vectors $|\phi_1\rangle$ and $|\phi_2\rangle$ will be θ. Since $E_{ij} = \langle\phi| A_i B_j |\phi\rangle$, from the fact that $E_{00} = 1$, we know that

$$A_0 |\phi\rangle = B_0 |\phi\rangle \, . \tag{2.9}$$

Similarly, we can infer that

$$\begin{gathered} A_1 |\phi\rangle = B_1 |\phi\rangle \, , \\ A_0 |\phi\rangle \perp B_1 |\phi\rangle \, , \qquad A_1 |\phi\rangle \perp B_0 |\phi\rangle \, , \\ \theta(A_2 |\phi\rangle \, , B_0 |\phi\rangle) = \frac{\pi}{4}, \qquad \theta(A_2 |\phi\rangle \, , B_1 |\phi\rangle) = \frac{\pi}{4}. \end{gathered} \tag{2.10}$$

To achieve the above relations, the only possibility is that the vector $A_2 |\phi\rangle$ lies in the middle of the vectors $A_0 \left|\phi\right\rangle$ and $A_1 \left|\phi\right\rangle$, which simply means,

$$A_2 \left|\phi\right\rangle = \frac{A_0 + A_1}{\sqrt{2}} \left|\phi\right\rangle = \frac{B_0 + B_1}{\sqrt{2}} \left|\phi\right\rangle . \tag{2.11}$$

If one multiply A_2 on the left of both side,

$$\begin{aligned} \text{l.h.s} &= A_2^2 \left|\phi\right\rangle = \left|\phi\right\rangle , \\ \text{r.h.s} &= A_2 \frac{B_0 + B_1}{\sqrt{2}} \left|\phi\right\rangle \\ &= \frac{B_0 + B_1}{\sqrt{2}} A_2 \left|\phi\right\rangle = \left(\frac{B_0 + B_1}{\sqrt{2}}\right)^2 \left|\phi\right\rangle \\ &= \frac{1}{2} \left(B_0^2 + B_1^2 + B_0 B_1 + B_1 B_0\right) \left|\phi\right\rangle , \end{aligned} \tag{2.12}$$

with the property $A_i^2 = B_j^2 = \mathbb{1}$, we get the following relation immediately

$$\left(B_0 B_1 + B_1 B_0\right) \left|\phi\right\rangle = 0. \tag{2.13}$$

This is nothing but the anti-commutative property of B_0 and B_1. With similar calculations, we could also derive that

$$\left(A_0 A_1 + A_1 A_0\right) \left|\phi\right\rangle = 0. \tag{2.14}$$

With these properties of A_i and B_j, we could already construct a local isometry Ψ as in Figure 2.1.

What the isometry does is to extract the target state $\left|\Phi^+\right\rangle$ out of the system into

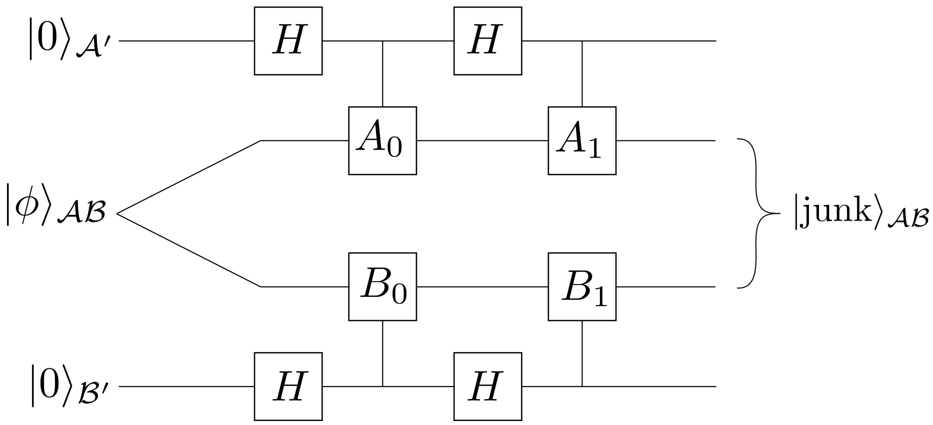

$|0\rangle_{\mathcal{A}'}$
H
H
A_0
A_1
$|\phi\rangle_{\mathcal{AB}}$
$|\text{junk}\rangle_{\mathcal{AB}}$
B_0
B_1
$|0\rangle_{\mathcal{B}'}$
H
H

Figure 2.1: Local isometry that extracts the target state from the system into the ancillary qubits. H is the qubit Hadamard gate.

the ancillary qubits. To see this more clearly, we practice the following exercise,

$$
\begin{aligned}
&\Psi(|\phi\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A}'\mathcal{B}'}) = \mathrm{C}_{A_1}\mathrm{C}_{B_1}\mathcal{H}_{\mathcal{A}'}\mathcal{H}_{\mathcal{B}'}\mathrm{C}_{A_0}\mathrm{C}_{B_0}\mathcal{H}_{\mathcal{A}'}\mathcal{H}_{\mathcal{B}'}\,|\phi\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A}'\mathcal{B}'} \\
=&\mathrm{C}_{A_1}\mathrm{C}_{B_1}\mathcal{H}_{\mathcal{A}'}\mathcal{H}_{\mathcal{B}'}\mathrm{C}_{A_0}\mathrm{C}_{B_0}\,|\phi\rangle_{\mathcal{AB}} \otimes |{+}{+}\rangle_{\mathcal{A}'\mathcal{B}'} \\
=&\frac{1}{2}\mathrm{C}_{A_1}\mathrm{C}_{B_1}\mathcal{H}_{\mathcal{A}'}\mathcal{H}_{\mathcal{B}'}(|\phi\rangle_{\mathcal{AB}}\,|00\rangle_{\mathcal{A}'\mathcal{B}'} + B_0\,|\phi\rangle_{\mathcal{AB}}\,|01\rangle_{\mathcal{A}'\mathcal{B}'} \\
&+ A_0\,|\phi\rangle_{\mathcal{AB}}\,|10\rangle_{\mathcal{A}'\mathcal{B}'} + A_0B_0\,|\phi\rangle_{\mathcal{AB}}\,|11\rangle_{\mathcal{A}'\mathcal{B}'}) \\
=&\frac{1}{2}\mathrm{C}_{A_1}\mathrm{C}_{B_1}(|\phi\rangle_{\mathcal{AB}}\,|{+}{+}\rangle_{\mathcal{A}'\mathcal{B}'} + B_0\,|\phi\rangle_{\mathcal{AB}}\,|{+}{-}\rangle_{\mathcal{A}'\mathcal{B}'} \\
&+ A_0\,|\phi\rangle_{\mathcal{AB}}\,|{-}{+}\rangle_{\mathcal{A}'\mathcal{B}'} + A_0B_0\,|\phi\rangle_{\mathcal{AB}}\,|{-}{-}\rangle_{\mathcal{A}'\mathcal{B}'}) \\
=&\frac{1}{4}[(\mathbb{1} + A_0)(\mathbb{1} + B_0)\,|\phi\rangle_{\mathcal{AB}}\,|00\rangle_{\mathcal{A}'\mathcal{B}'} + B_1(\mathbb{1} + A_0)(\mathbb{1} - B_0)\,|\phi\rangle_{\mathcal{AB}}\,|01\rangle_{\mathcal{A}'\mathcal{B}'} \\
&+ A_1(\mathbb{1} - A_0)(\mathbb{1} + B_0)\,|\phi\rangle_{\mathcal{AB}}\,|10\rangle_{\mathcal{A}'\mathcal{B}'} + A_1B_1(\mathbb{1} - A_0)(\mathbb{1} - B_0)\,|\phi\rangle_{\mathcal{AB}}\,|11\rangle_{\mathcal{A}'\mathcal{B}'}],
\end{aligned}
\tag{2.15}
$$

where C_{A_i/B_j} represents the control gate of A_i or B_j and $\mathcal{H}$ represents the Hadamard gate, and $|\pm\rangle$ represents the state $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$. One could check that in fact the isometry we used here is local and unitary, which are the conditions that any real isometry should satisfy. With the help of properties (2.9), (2.10), (2.13) and (2.14), it will not be difficult to proceed with the simplification of the above equation

$$\begin{aligned}\Psi(|\phi\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A}'\mathcal{B}'}) &= \frac{1}{2}(\mathbb{1} + A_0)\,|\psi\rangle_{\mathcal{AB}}\,(|00\rangle + |11\rangle)_{\mathcal{A}'\mathcal{B}'} \\ &= \frac{\mathbb{1} + A_0}{\sqrt{2}}\,|\psi\rangle_{\mathcal{AB}}\,|\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'}\,. \end{aligned} \tag{2.16}$$

This is exactly what the definition of self-testing is as (2.4). The part of $\frac{\mathbb{1}+A_0}{\sqrt{2}}\,|\psi\rangle_{\mathcal{AB}}$ would be the junk state. For the condition (2.5), it is not hard to see once we plug the operators in equation (2.15). □

With the example of the Mayers-Yao test, we can now have a summary of the self-testing of the singlet state.

Theorem 3. *For the two qubit singlet state $|\Phi^+\rangle_{\mathcal{AB}}$, a self-testing is possible if one can define unitary operators Z_A, X_A, Z_B and X_B, such that*

$$Z_A\,|\phi\rangle = Z_B\,|\phi\rangle\,, \tag{2.17}$$

$$Z_A X_A\,|\phi\rangle = -X_A Z_A\,|\phi\rangle\,, \tag{2.18}$$

$$Z_B X_B\,|\phi\rangle = -X_B Z_B\,|\phi\rangle\,. \tag{2.19}$$

2.2 Robustness

One of the main issue for self-testing is that whether it is robust against statistic errors. The problem is interesting simply because we can never have perfect statistics in the real case. Hence, it remains to be answered whether the state of the system is close to the ideal state even if the statistics is not perfect, and also how much it is close to.

Once the system we are studying is not ideal, basically all the equations in the *Proof* of Theorem 2 will not be valid. All the nice relations between the operators and the anti-commutative relations do not hold any more. However, the optimistic fact is that the isometry we defined in the ideal case is still a valid isometry, in the sense that it is local and unitary. Thus, it is no harm if we apply the same isometry as we had in the ideal self-testing to the non-ideal one. It is for sure that the output state after the isometry will be different compared to the ideal one, and the distance between these two is what we are interested in.

To continue the discussion of robustness, we will use the example of Mayers-Yao again. For clarity, we will denote the system that corresponds to the ideal statistics from now on as $|\tilde{\phi}\rangle$. The distance between the output of the isometry for the real system and the ideal one is

$$D = \|\Psi(|\phi\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A}'\mathcal{B}'}) - \Psi(|\tilde{\phi}\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A}'\mathcal{B}'})\|. \tag{2.20}$$

If we consider the case that the errors of all the statistics are upper bounded by ϵ, which is

$$\|p(ab|xy) - \tilde{p}(ab|xy)\| \leq \epsilon, \tag{2.21}$$

where $\tilde{p}$ corresponds to the ideal case. Then it would be nice to show that the distance D is upper bounded by some function of ϵ

$$D \leq f(\epsilon), \tag{2.22}$$

and the performance of self-testing depends on the scaling of the function $f(\epsilon)$.

With tedious calculations, one could derive that

$$f(\epsilon) = \sqrt{2}\epsilon + 2\sqrt{2}(\sqrt{2}\epsilon)^{\frac{1}{4}}. \tag{2.23}$$

as given in [52].

2.3 Self-testing with inequalities

In the example of the Mayers-Yao test, it uses the probability distribution as a criterion to self-test. In fact, the inequalities arise from the game could also be used as criteria as shown in [52]. In this section, we will go over these results to see how it is done.

Basically, it is going to be the same state, which is the maximally entangled state. Instead of having three measurements on Alice side, now he only has two. One could still use $x, y \in \{0, 1\}$ to denote the inputs and $a, b \in \{0, 1\}$ to denote the outputs. The inequality that will be used is the CHSH inequality as shown in Chapter 1. The self-testing of the CHSH inequality says:

Theorem 4. *If the CHSH inequality (1.3) is maximally violated by $2\sqrt{2}$, there exists a local isometry $\Psi = \Psi_A \otimes \Psi_B$, such that for the state of the device $|\phi\rangle$ and the measurements A_i, B_j:*

$$\Psi(|\phi\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A}'\mathcal{B}'}) = |junk\rangle_{\mathcal{AB}} \otimes |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'}\,, \tag{2.24}$$

$$\Psi(A_i B_j |\phi\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A}'\mathcal{B}'}) = |junk\rangle_{\mathcal{AB}} \otimes (\sigma_i \otimes \sigma_j) |\Phi^+\rangle_{\mathcal{A}'\mathcal{B}'}\,, \tag{2.25}$$

where σ-s are the Pauli operations on the ancillary qubits.

Proof. Here, we will not go through the complete proof, since we only need to define unitary measurements X_A, X_B, Z_A and Z_B that satisfy

$$\begin{aligned} X_A |\phi\rangle &= X_B |\phi\rangle\,, & Z_A |\phi\rangle &= Z_B |\phi\rangle\,, \\ X_A Z_A |\phi\rangle &= -Z_A X_A |\phi\rangle\,, & X_B Z_B |\phi\rangle &= -Z_B X_B |\phi\rangle\,. \end{aligned} \tag{2.26}$$

Once we have these measurements properly defined, a self-testing will following naturally as what we did in the Mayers-Yao example.

To show the existence of such measurements, let us try to define them as below first.

$$\begin{aligned} Z_A &= A_0, & X_A &= A_1, \\ Z_B &= \frac{B_0 + B_1}{|B_0 + B_1|}, & X_B &= \frac{B_0 - B_1}{|B_0 - B_1|}, \end{aligned} \tag{2.27}$$

where $|B_0 \pm B_1| = \sqrt{(B_0 \pm B_1)^2}$. With such definition, we could see that X_A, X_B, Z_A

and Z_B are all unitary.

The maximal violation of CHSH basically tells us

$$\begin{aligned}
&\langle\phi|\, A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1\, |\phi\rangle \\
=&\langle\phi|\, A_0(B_0 + B_1) + A_1(B_0 - B_1)\, |\phi\rangle \\
=&2\sqrt{2}.
\end{aligned} \tag{2.28}$$

Let us first try to evaluate the norm of the following vectors

$$\|\big(A_0 - (B_0 + B_1)/\sqrt{2}\big)\, |\phi\rangle\, \| = \sqrt{2 + \langle\phi|\, \{B_0, B_1\}/2\, |\phi\rangle - \sqrt{2}\, \langle\phi|\, A_0(B_0 + B_1)\, |\phi\rangle}, \tag{2.29}$$

$$\|\big(A_1 - (B_0 - B_1)/\sqrt{2}\big)\, |\phi\rangle\, \| = \sqrt{2 - \langle\phi|\, \{B_0, B_1\}/2\, |\phi\rangle - \sqrt{2}\, \langle\phi|\, A_1(B_0 - B_1)\, |\phi\rangle}. \tag{2.30}$$

This will simply imply that

$$\langle\phi|\, A_0(B_0 + B_1)\, |\phi\rangle \leq \sqrt{2} + \langle\phi|\, \{B_0, B_1\}/2\sqrt{2}\, |\phi\rangle\,, \tag{2.31}$$

$$\langle\phi|\, A_1(B_0 - B_1)\, |\phi\rangle \leq \sqrt{2} - \langle\phi|\, \{B_0, B_1\}/2\sqrt{2}\, |\phi\rangle\,. \tag{2.32}$$

However, according to the CHSH violation (2.28), the sum of the two term must be $2\sqrt{2}$. It then follows that

$$\langle\phi|\, A_0(B_0 + B_1)\, |\phi\rangle = \sqrt{2} + \langle\phi|\, \{B_0, B_1\}/2\sqrt{2}\, |\phi\rangle \tag{2.33}$$

$$\langle\phi|\, A_1(B_0 - B_1)\, |\phi\rangle = \sqrt{2} - \langle\phi|\, \{B_0, B_1\}/2\sqrt{2}\, |\phi\rangle\,, \tag{2.34}$$

If we apply Cauchy-Schwartz inequality to (2.33) and (2.34), we get

$$\langle\phi|\, A_0(B_0 + B_1)\, |\phi\rangle \leq \langle\phi|\, |A_0(B_0 + B_1)|\, |\phi\rangle \leq \langle\phi|\, |B_0 + B_1|\, |\phi\rangle\,, \tag{2.35}$$

$$\langle\phi|\, A_1(B_0 - B_1)\, |\phi\rangle \leq \langle\phi|\, |A_1(B_0 - B_1)|\, |\phi\rangle \leq \langle\phi|\, |B_0 - B_1|\, |\phi\rangle\,, \tag{2.36}$$

which is

$$|B_0 + B_1| \geq \sqrt{2} + \langle\phi| \{B_0, B_1\}/2\sqrt{2} \, |\phi\rangle \, , \tag{2.37}$$

$$|B_0 - B_1| \geq \sqrt{2} - \langle\phi| \{B_0, B_1\}/2\sqrt{2} \, |\phi\rangle \, . \tag{2.38}$$

We can square both inequalities and get

$$2 + \{B_0, B_1\} \geq 2 + \langle\phi| \{B_0, B_1\}/2\sqrt{2} \, |\phi\rangle^2 + \langle\phi| \{B_0, B_1\} |\phi\rangle \, , \tag{2.39}$$

$$2 - \{B_0, B_1\} \geq 2 + \langle\phi| \{B_0, B_1\}/2\sqrt{2} \, |\phi\rangle^2 - \langle\phi| \{B_0, B_1\} |\phi\rangle \, . \tag{2.40}$$

Evaluating both side of the above inequalities on state $|\phi\rangle$, we get

$$2 + \langle\phi| \{B_0, B_1\} |\phi\rangle \geq 2 + \langle\phi| \{B_0, B_1\}/2\sqrt{2} \, |\phi\rangle^2 + \langle\phi| \{B_0, B_1\} |\phi\rangle \, , \tag{2.41}$$

$$2 - \langle\phi| \{B_0, B_1\} |\phi\rangle \geq 2 + \langle\phi| \{B_0, B_1\}/2\sqrt{2} \, |\phi\rangle^2 - \langle\phi| \{B_0, B_1\} |\phi\rangle \, . \tag{2.42}$$

To make the above inequalities hold, it must be satisfied that,

$$\langle\phi| \{B_0, B_1\} |\phi\rangle = 0. \tag{2.43}$$

Thus, $|B_0 + B_1| = |B_0 - B_1| = \sqrt{2}$ and,

$$\{B_0, B_1\} = 0. \tag{2.44}$$

From (2.33) and (2.34), we will see that

$$Z_A \, |\phi\rangle = A_0 \, |\phi\rangle = \frac{B_0 + B_1}{\sqrt{2}} \, |\phi\rangle \, , \tag{2.45}$$

$$X_A \, |\phi\rangle = A_1 \, |\phi\rangle = \frac{B_0 - B_1}{\sqrt{2}} \, |\phi\rangle \, . \tag{2.46}$$

Hence $Z_B = \frac{B_0+B_1}{\sqrt{2}}$ and $X_B = \frac{B_0-B_1}{\sqrt{2}}$, besides

$$Z_A \left|\phi\right\rangle = Z_B \left|\phi\right\rangle , \tag{2.47}$$

$$X_A \left|\phi\right\rangle = X_B \left|\phi\right\rangle . \tag{2.48}$$

The commutation relation will follow immediately

$$X_B Z_B + Z_B X_B = \frac{1}{2}(B_1 B_0 - B_0 B_1) + \frac{1}{2}(B_0 B_1 - B_1 B_0) = 0. \tag{2.49}$$

Hence

$$\begin{aligned}(X_A Z_A + Z_A X_A) \left|\phi\right\rangle &= (X_A Z_B + Z_A X_B) \left|\phi\right\rangle \\ =&(Z_B X_A + X_B Z_A) \left|\phi\right\rangle = (Z_B X_B + X_B Z_B) \left|\phi\right\rangle = 0. \end{aligned} \tag{2.50}$$

With the unitary operators X_A, X_B, Z_A and Z_B equipped with the properties (2.47), (2.48), (2.49) and (2.50), we can then follow what we did in the Mayers-Yao example and complete the proof. □

2.4 Self-testing with semidefinite program

Although the way we dealt with the robustness bounds in the previous section is useful, sometimes the scaling of the function $f(\epsilon)$ may not be that good. Normally, the best bound we could get scales like $O(\epsilon^{\frac{1}{2}})$ and sometimes even worse as $O(\epsilon^{\frac{1}{8}})$ [60, 52, 54]. This will impose a higher requirement on the experiments. Even though, with the state of art experiment that is dedicated to this kind of test, the performance of the bound is still reasonable, we still hope to find out whether it is possible to improve the robustness bounds or not.

Semidefinite program (SDP) has been used a lot to tackle the problems in the study of quantum mechanics, for instance, the characterization the set of separable states [61, 62], bounding the amount of randomness [27, 28], state discrimination [63] and etc. Self-testing with semidefinite program (SDP) has recently been developed to tackle this problem [31, 32]. In terms of robustness performance, it improves a lot over the analytical methods we were using in the previous section. However, it should be emphasized that the best thing about this idea is not just to improve the robustness, but to give a new way of how we think about self-testing.

Let us take a look at the Definition 2 of self-testing, for a general state that may not be the ideal case, as we have said before, there is no harm to apply the same isometry as we had in the ideal self-testing to the non-ideal one,

$$\Psi(|\phi\rangle_{\mathcal{AB}} \otimes |\xi\rangle_{\mathcal{A}'\mathcal{B}'}) = |\text{junk}\rangle_{\mathcal{AB}} \otimes |\varphi\rangle_{\mathcal{A}'\mathcal{B}'} .$$

As long as the isometry is local and unitary, this operation is valid. Even though there might be isometries that could have better performance, we still stay our focus on the above isometry since it will give a lower bound of all possible isometries. If this isometry leads to a better robustness bound, our aim has already been achieved. However, this will not forbid one to study possible alternatives of isometries. We will use the fidelity to measure the distance between the ideal system and the nonideal one is

$$F = \parallel \langle\tilde{\varphi}|\varphi\rangle_{\mathcal{A}'\mathcal{B}'} \parallel^2, \tag{2.51}$$

where $|\varphi\rangle_{\mathcal{A}'\mathcal{B}'}$ is the state of the ancillary qubits after tracing out the system, and $|\tilde{\varphi}\rangle$ is the ideal target state that we are trying to self-test the system into. With the isometry which we have described in Figure 2.1, Ψ could be expressed as a linear combination of the measurement operators and the fidelity F then could always be expressed as a linear function of the average values of the measurement operator monomials. This could be seen from (2.15) for example. In (2.15), after $\mathcal{AB}$ are traced out, the coefficients of $|ij\rangle_{\mathcal{A}'\mathcal{B}'}$ will be sums of the average values of the measurement operator monomials. Thus, one will get a linear function of the average values of the measurement operator monomials if the fidelity of the ancillary qubits with the target state is calculated. These monomials are simply the elements of a sequence S defined in Chapter 1.

$$S = \{\mathbb{1}\} \cup \{\Pi_{a|x}\} \cup \{\Pi_{b|y}\} \cup \{\Pi_{a|x}\Pi_{a'|x'}\} \cup \{\Pi_{b|y}\Pi_{b'|y'}\} \cup \{\Pi_{a|x}\Pi_{b|y}\} \ldots .$$

Since the experiment only gives us the knowledge about the probability distribution but not the terms like $\Pi_{a|x}\Pi_{a'|x'}$, the problem left is to find out the values of those unknown operator monomials that are allowed by quantum mechanics. Such a problem could be cast into the following semidefinite program

$$\begin{aligned} \min \quad & F(S) \\ \text{such that} \quad & \langle\phi| \Pi_{a|x}\Pi_{b|y} |\phi\rangle_{\mathcal{AB}} = p(ab|xy), \\ & \Gamma \geq 0, \end{aligned} \tag{2.52}$$

where $\Gamma(S)$ is a *certificate* defined in Chapter 1. As we have shown a certain monomials *certificate*, $\Gamma(S^n) \geq 0$ is a relaxation of the requirement that the behaviour of the system belongs to quantum mechanics. Hence, a looser condition will give us a valid lower bound of the fidelity F, which is also the robustness bound of the self-testing.

There are two essential factors of this method. Firstly, we need to have a proper probability distribution as a criterion. Secondly, with this criterion, we need to define an isometry corresponding to the closest ideal case self-testing compared with the real one. The isometry is the key to derive the expression of fidelity F. With these two factors fulfilled, it is then possible to solve the SDP (2.52). It is also these factors that we will dedicate the main efforts to in the self-testings that will appear later in this thesis.

2.5 By-products of self-testing with SDP

The SDP method provides us a novel perspective of how we view self-testing. Compared to the methods we introduced earlier, it simplifies the way we solve the problem and improves the robustness a lot. However, these are not the only benefits we get from self-testing with SDP. We are going to discuss these by-products of self-testing with SDP in two aspects here. The first one is to derive an inequality that is maximally violated by the state $|\tilde{\varphi}\rangle$ that is self-tested, which has been shown in [64]. The second one is to retrieve the quantum strategy that achieves the probability $p(ab|xy)$ that is used as the criterion to self-test as given in [11].

To begin with, let us first introduce the duality theory. Generally, a semidefinite problem could be formalized in the following way

$$\begin{aligned} \min_{X} \quad & \langle C, X\rangle \\ \text{subject to} \quad & \langle A_k, X\rangle = b_k, \qquad k = 1, 2, ..., m, \\ & X \geq 0, \end{aligned} \tag{2.53}$$

where C and X are matrices, and $\langle C, X\rangle = \mathrm{Tr}[C^T X]$. It is normally called the primal problem. On the contrary, there exists a counterpart problem that is called the dual problem, which takes the form

$$\begin{aligned} \max_{y} \quad & \textstyle\sum_k b_k y_k \\ \text{subject to} \quad & \textstyle\sum_k y_k A_k - C \leq 0, \qquad k = 1, 2, ..., m. \end{aligned} \tag{2.54}$$

Therefore the SDP of self-testing maps to the formalism of the primal problem and $p(ab|xy)$ will be the b_ks. With such formalism of the primal and dual problem, there are the weak duality theorem and strong duality theorem which can be proved. The weak duality theorem states that,

Theorem 5. *if both the primal and dual problems are feasible, the value of the primal SDP is at least the value of the dual SDP.*

Proof. The proof is quite straight forward.

$$\langle C, X\rangle - \sum_k b_k y_k = \langle C, X\rangle - \sum_k y_k \langle A_k, X\rangle = \langle C - \sum_k y_k A_k, X\rangle \geq 0. \tag{2.55}$$

□

The above value is normally referred as the *duality gap*. Besides, the strong duality theorem says,

Theorem 6. *if the primal problem is bounded and strictly feasible ($X > 0$), then the dual problem has a optimal solution and $\langle C, X\rangle = \sum_k b_k y_k$, and vice versa. If both the primal and dual problem are bounded and strictly feasible, both problems will have optimal solutions.*

The proofs of the above two theorems could be found in [65]. The weak and strong duality theorems basically tell us that, if a self-testing SDP has optimal solutions for both the primal and dual problems, the objective functions of the two problems will be equal. Since the primal and dual problem are equivalent, y_ks are also constrained by quantum physics. Noticing that in the objective function of the dual problem, b_ks are actually the probability distribution, then the dual problem is basically doing the maximization over any linear combination of the given probability distribution over the quantum mechanically allowed space in y_ks. It is now clear that this specific linear combination of $p(ab|xy)$s that achieves the maximum is the inequality we are looking for. To put it neatly

$$\mathcal{I} = \sum_k y_k^* p_k(ab|xy), \tag{2.56}$$

where y_k^* represents the value of the variable which gives the optimal solution of the SDP and $p_k(ab|xy)$ is the corresponding probability term to b_k.

The other by-product we are going to talk about here is the reconstruction of the quantum strategy that achieves $p(ab|xy)$ given the SDP is optimally solved. This only make sense if the system really belongs to quantum. However, as we have shown in Chapter 1, generally, the size of the SDP problem goes to infinite in order to achieve the quantum set. Therefore, this seems to be a no-go path to what we need practically. Fortunately, there are some cases that we may still do something.

Theorem 7. *Suppose $\Gamma^n_{X,Y} = \{\Gamma^n_{s,t} : s,t \in S_{X,Y}\}$ is a submatrix of Γ^n, where $S_{X,Y} = \{s : |s| \leq n^* - 1\} \cup \{s : s = abs', a \in X, b \in Y, s' \in S_{X,Y}, |s| \leq n^*\}$ and $n^* < n$. For a finite n, if there exists some n^*, such that*

$$rank(\Gamma^n_{X,Y}) = rank(\Gamma^n), \tag{2.57}$$

for all X, Y, the behaviour $p(ab|xy)$ has a quantum representation with a Hilbert space dimension $d \geq$ rank(Γ^n).

This basically tells us that if the *certificate* matrix is not full rank in a way that is described in the above theorem, we can always find a finite dimensional quantum system and measurement settings that achieve $p(ab|xy)$. However, we are not going to show all the details here. For more information about the proof and the techniques to reconstruct the state and measurements, please refer to [11].

Chapter 3

Self-testing of bipartite systems

In this chapter, we are going to talk about the self-testing of bipartite systems. Bipartite quantum systems are broadly used in quantum information processing, for instance, quantum key distribution [35, 36, 37, 38, 39, 40], quantum random generation [27, 28], certification of entangled measurements [66], quantum repeaters [67, 68] and etc. Hence, it is important to assure that the bipartite systems used in these tasks are what they are required to be, especially for those tasks that the customers really have no access to the inner mechanism of the devices. Self-testing provides a device-independent way to certify the state and measurements. It only requires the experimental statistics. The self-testing of bipartite state is also the best studied case. Here, we will first focus on the maximally entangled state and see a variety of the ways to self-test the same state. In this process, we found that a geometric view of this problem actually simplified most of the proofs a lot [57]. Then, we will talk a bit more on the self-testing of an arbitrary bipartite state. Furthermore, we will have some outlooks on the future study of self-testing of bipartite systems.

3.1 Self-testing of singlet state

The singlet state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, also called maximally entangled state, is the most encountered state in quantum information processing. A lot of protocols and tasks utilize the nice properties of this state to make it possible to achieve quantum advantages over classical systems. Due to this fact, the progress of self-testing's history is actually accompanied by the development of the self-testing of the singlet state. The first work that contains the idea of self-testing the singlet state was given by Popescu and Rohrlich in 1992 [49], later in 2004, Mayers and Yao first coined the task to certify imperfect apparatuses as 'self-testing' [51]. However, till that time, robustness of self-testing is still not considered for practical usage. In 2012, Mckague et al. [52] simplified the proof of the original self-testing of the singlet state and made it robust against experimental fluctuations for the first time.

Since we have used the self-testing of the singlet state in Chapter 2 to introduce the general formalism of self-testing, we will not show it again here. One could also refer back to Chapter 2 for more details about these two tests.

3.2 All the self-testings of singlet state

A short summary for the self-testing of the singlet state is, till 2012, the ways to self-test are basically the CHSH test and the Mayers-Yao test. These two ways of self-testing the singlet state are different in the sense that the probability arising from the two tests are not equivalent. If we consider them as points in the probability space $\mathcal{P}$, they are two distinct points at different locations. This inspires us that possibly there are more criteria which can also self-test the singlet state. Moreover, is it possible to make a connection between these two points in a certain way such that all the points belongs to the connection self-test the singlet state?

The answer to these questions turn out to be yes and there are actually a lot more criteria that coincide with our expectations. We call this result as all the self-testings of the singlet state [57]. In the process of deriving this result, we also found a geometric way to look into the self-testing problem, which has never been used before. It gives us a more intuitive view on the nature of the problem rather than mathematical equations.

As we have seen in Chapter 2, the most important factor of self-testing is to define a valid local isometry that extracts the target state out of the system. From Theorem

3, we see that as soon as one could find unitary operators $X_{A/B}$ and $Z_{A/B}$, we call them control operators, on each party such that

$$\begin{aligned} X_A\left|\phi\right\rangle &= X_B\left|\phi\right\rangle, & Z_A\left|\phi\right\rangle &= Z_B\left|\phi\right\rangle, \\ X_A Z_A\left|\phi\right\rangle &= -Z_A X_A\left|\phi\right\rangle, & X_B Z_B\left|\phi\right\rangle &= -Z_B X_B\left|\phi\right\rangle, \end{aligned} \tag{3.1}$$

the isometry could be immediately constructed as in Figure 2.1. The construction of the control operators $X_{A/B}$ and $Z_{A/B}$ should be purely based on the knowledge we had for the system, which are the measurements $\{\Pi_{a|x}\}, \{\Pi_{b|y}\}$ and the probability distribution $p(ab|xy)$.

3.2.1 All the self-testings in the ideal case

We state the result as the following.

Theorem 8. *A and B both choose one dichotomic measurement out of two and we denote their choices as $x \in \{0,1\}$ and $y \in \{0,1\}$. The outputs of A and B will be denoted by $a \in \{0,1\}$ and $b \in \{0,1\}$. The observed correlation E_{xy} will self-test a singlet state if and only if*

$$\sum_{(x,y)\neq(i,j)} \arcsin(E_{xy}) - \arcsin(E_{ij}) = \xi\pi \quad \textit{with } i,j \in \{0,1\},\, \xi \in \{+1,-1\}, \tag{3.2}$$

where $\arcsin(E_{xy}) \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, *and provided* $\arccos(E_{xy}) = 0$ *or* π *holds for at most one pair* (x,y).

Proof. First we should stress that if there are more than one $\arccos(E_{xy})$ equal to 0 or π, one could actually check that the correlations arising from this case will be local. Hence there is no need to consider the self-testing of this case.

We will now prove that (3.2) is a sufficient condition for self-testing the singlet state. The measurement operators involved in this problems are A_0, A_1, B_0 and B_1, which are defined as

$$
\begin{aligned}
A_x &= \Pi_{0|x} - \Pi_{1|x}, \\
B_y &= \Pi_{0|y} - \Pi_{0|y}.
\end{aligned}
\tag{3.3}
$$

They are all unitary and hence satisfy $A_x^2 = B_y^2 = \mathbb{1}$. The vectors representing $A_x |\phi\rangle$ and $B_y |\phi\rangle$ live in a space with unbounded dimension. However, these vectors satisfy the following relations

$$
\langle A_x |\phi\rangle , B_y |\phi\rangle\rangle = E_{xy},
\tag{3.4}
$$

where $\langle \vec{u}, \vec{v}\rangle$ is the inner product of $\vec{u}$ and $\vec{v}$. Let us denote $E_{xy} = \cos \alpha_{xy}$, where $\alpha_{xy} \geq 0$. α_{xy} basically represents the angle spanned by vectors $A_x |\phi\rangle$ and $B_y |\phi\rangle$.

Let us first consider the relations between the vectors $A_0 |\phi\rangle$, $A_1 |\phi\rangle$ and $B_0 |\phi\rangle$. From the simple reason that the angle spanned by $A_0 |\phi\rangle$ and $A_1 |\phi\rangle$ will be smaller than the sum of the angles spanned by $A_0 |\phi\rangle$ with $B_0 |\phi\rangle$ and $A_1 |\phi\rangle$ with $B_0 |\phi\rangle$, and larger than the difference of the two, we get

$$
|\alpha_{00} - \alpha_{10}| \leq \theta \leq \alpha_{00} + \alpha_{10},
\tag{3.5}
$$

where $\theta = \langle A_0 |\phi\rangle , A_1 |\phi\rangle\rangle$. We can also argue similarly for the vectors $A_0 |\phi\rangle$, $A_1 |\phi\rangle$ and $B_1 |\phi\rangle$ and get

$$
|\alpha_{01} - \alpha_{11}| \leq \theta \leq \alpha_{01} + \alpha_{11}.
\tag{3.6}
$$

In fact, the eight conditions (3.2) are equivalent to each other after relabelling of the input and output indexes. Hence, it is reasonable to assume $\arcsin(E_{00}) + \arcsin(E_{01}) + \arcsin(E_{10}) - \arcsin(E_{11}) = \pi$, which means

$$
\alpha_{00} + \alpha_{10} = \alpha_{01} - \alpha_{11}.
\tag{3.7}
$$

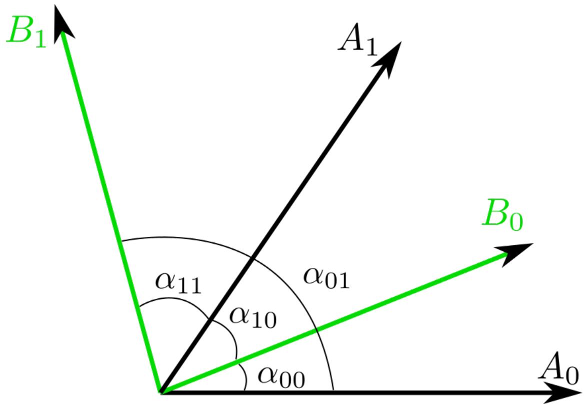


Figure 3.1: Relative configuration of the vectors.

Now it is clear that (3.5) and (3.6) could be satisfied if and only if

$$\theta = \alpha_{00} + \alpha_{10} = \alpha_{01} - \alpha_{11}. \tag{3.8}$$

To this point, all the four vectors $A_x\,|\phi\rangle$ and $B_y\,|\phi\rangle$ could be decided in the same space, as sketched in Figure 3.1. It is not difficult to derive that

$$B_0|\phi\rangle = \frac{\sin(\alpha_{00})A_1|\phi\rangle + \sin(\alpha_{10})A_0|\phi\rangle}{\sin(\alpha_{00}+\alpha_{10})}, \tag{3.9}$$

$$A_1|\phi\rangle = \frac{\sin(\alpha_{10})B_1|\phi\rangle + \sin(\alpha_{11})B_0|\phi\rangle}{\sin(\alpha_{11}+\alpha_{10})}. \tag{3.10}$$

Due to the fact that $A_x^2 = B_y^2 = \mathbb{1}$ and $[A_x, B_y] = 0$, after we apply B_0 on (3.9), we get

$$\begin{aligned} B_0^2|\phi\rangle &= B_0\frac{\sin(\alpha_{00})A_1|\phi\rangle + \sin(\alpha_{10})A_0|\phi\rangle}{\sin(\alpha_{00}+\alpha_{10})} \\ &= \frac{\sin(\alpha_{00})A_1 + \sin(\alpha_{10})A_0}{\sin(\alpha_{00}+\alpha_{10}))}B_0|\phi\rangle \;=\; \left(\frac{\sin(\alpha_{00})A_1 + \sin(\alpha_{10})A_0}{\sin(\alpha_{00}+\alpha_{10})}\right)^2|\phi\rangle \\ &= \frac{\sin^2(\alpha_{00}) + \sin^2(\alpha_{10}) + \sin^2(\alpha_{00})\sin^2(\alpha_{10})(A_0A_1 + A_1A_0)}{\sin^2(\alpha_{00}+\alpha_{10})}\,|\phi\rangle\,, \end{aligned}$$

which infers

$$(A_0A_1 + A_1A_0)\,|\phi\rangle = 2\cos(\alpha_{00}+\alpha_{10})\,|\phi\rangle\,. \tag{3.11}$$

Similarly, we get

$$(B_0B_1 + B_1B_0)\left|\phi\right\rangle = 2\cos(\alpha_{10} + \alpha_{11})\left|\phi\right\rangle, \tag{3.12}$$

from (3.10). These commutation relation of A_x and B_y will help us to define the control operators

$$\begin{aligned} Z_A &= A_0, \\ X_A &= \frac{A_1 - \cos(\alpha_{00} + \alpha_{10})A_0}{\sin(\alpha_{00} + \alpha_{10})}, \\ Z_B &= \frac{\sin(\alpha_{01})B_0 - \sin(\alpha_{00})B_1}{\sin(\alpha_{01} - \alpha_{00})}, \\ X_B &= \frac{\sin(\alpha_{00})B_1 - \sin(\alpha_{01})B_0}{\sin(\alpha_{01} - \alpha_{00})}. \end{aligned} \tag{3.13}$$

We can actually check the commutation relation of $Z_{A/B}$ and $X_{A/B}$

$$\begin{aligned} &(Z_AX_A + X_AZ_A)\left|\phi\right\rangle \\ =&A_0\frac{A_1 - \cos(\alpha_{00} + \alpha_{10})A_0}{\sin(\alpha_{00} + \alpha_{10})}\left|\phi\right\rangle + \frac{A_1 - \cos(\alpha_{00} + \alpha_{10})A_0}{\sin(\alpha_{00} + \alpha_{10})}A_0\left|\phi\right\rangle \\ =&\frac{A_0A_1 + A_1A_0 - 2\cos(\alpha_{00} + \alpha_{10})}{\sin(\alpha_{00} + \alpha_10)}\left|\phi\right\rangle = 0. \end{aligned} \tag{3.14}$$

Similarly we can show that $(Z_BX_B + X_BZ_B)\left|\phi\right\rangle = 0$. Now, the only thing left to be proved is the unitarity of the operators (3.13). It is for sure that Z_A is unitary since A_0 is unitary by definition. For the rest, we will give the proof of X_A

$$\begin{aligned} \left\langle\phi\right| X_A^\dagger X_A \left|\phi\right\rangle &= \left\langle\phi\right| \frac{A_1^2 + \cos^2(\alpha_{00} + \alpha_{10})A_0^2 - \cos(\alpha_{00} + \alpha_{10})(A_0A_1 + A_1A_0)}{\sin^2(\alpha_{00} + \alpha_{10})}\left|\phi\right\rangle \\ &= 1, \end{aligned} \tag{3.15}$$

and the proof of Z_B and X_B will follow the same procedure. Besides, since $\left\langle\phi\right| Z_AZ_B \left|\phi\right\rangle =$

1 and $\langle\phi| X_A X_B |\phi\rangle = 1$, it follows that

$$\begin{aligned} Z_A |\phi\rangle &= Z_B |\phi\rangle \,, \\ X_A |\phi\rangle &= X_B |\phi\rangle \,. \end{aligned} \tag{3.16}$$

With the relations (3.14) and (3.16), we found the conditions for a self-testing as defined in (3.1) are satisfied. Hence, it would not be hard to show the self-testing following the standard method described in Chapter 2.

Now we will explain why (3.2) is a necessary condition to self-test the singlet state with the measurement scenario described in Theorem 8.

Firstly, it is widely known that the conditions (3.2) define the boundary of the correlations $\{E_{xy}\}$ achievable with quantum physics in the (2,2,2) scenario [2, 69]. Meanwhile, in the work of Masanes [70, 71], they proved that in a (2,2,2) scenario, an extremal point of the quantum set can be generated by measuring a singlet if and only if it satisfies (3.2). One could checked that the points satisfying condition (3.2) are all nonlocal except that more than one of the $\arccos(E_{xy})$ are zero or π. Since ideal self-testing is only achievable with points on the boundary of the quantum set, this suggests that any criterion that self-tests the singlet state must satisfy condition (3.2). □

With the results shown above, we found an interesting consequence [57]. The following correlations E_{xy} that self-test the singlet state

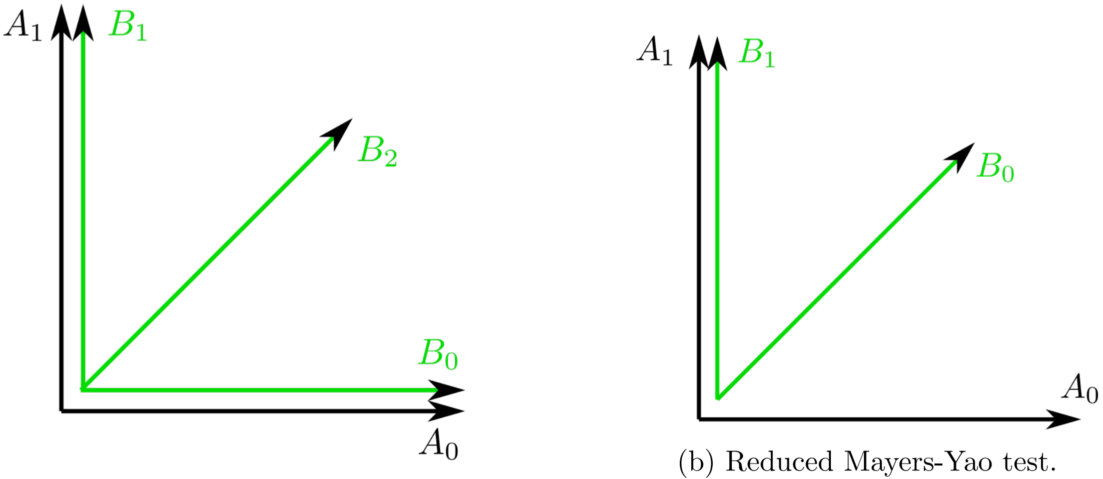
$$E_{00} = \frac{1}{\sqrt{2}}, \qquad E_{01} = 0, \tag{3.17}$$

$$E_{10} = \frac{1}{\sqrt{2}}, \qquad E_{11} = 1, \tag{3.18}$$

is just a simplification of the Mayers-Yao test, in which one of A's measurements is removed, see Figure 3.2. We call this as the reduced Mayers-Yao self-testing.

This suggest that the third measurement of A in the Mayers-Yao test is in fact redundant to achieve a self-testing of the singlet state.

One could also plot the area that could deliver a self-testing of the singlet state



(a) The original Mayers-Yao test.

(b) Reduced Mayers-Yao test.

Figure 3.2: The settings for the original Mayers-Yao test and the reduced Mayers-Yao test.

in the coordinates of αs. It is now able to put the simplified Mayers-Yao test and CHSH test in the same plot.

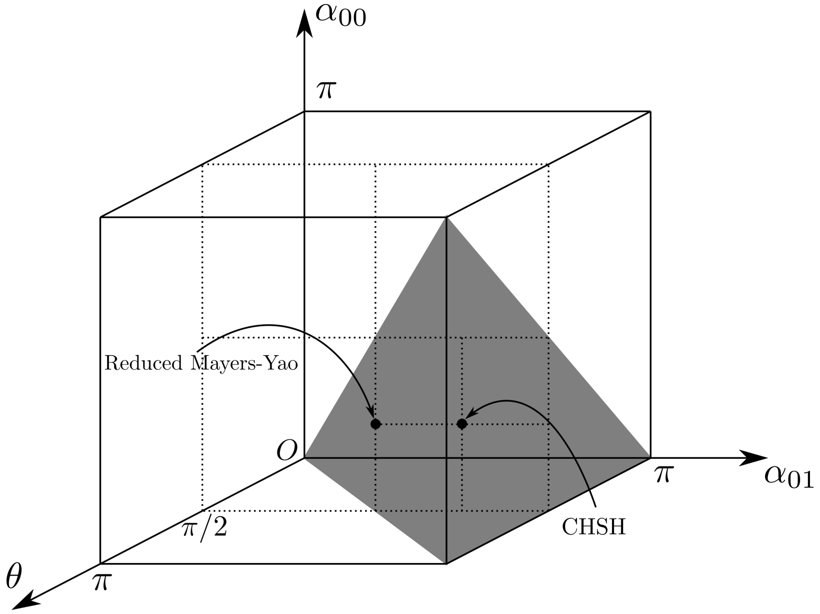


Figure 3.3: Regions in the space of αs (where we reduced the complexity of the problem by considering $\alpha_{00} + \alpha_{10} = \alpha_{01} - \alpha_{11}$) that can be self-tested, as the gray region.

3.2.2 Robustness

Next, we are going to discuss the robustness of such self-testings of the singlet state. As what we have discussed in Chapter 2, there are two treatments for the robustness of self-testing, analytical method and semidefinite programming method. Here, we will concentrate on the SDP method. The idea of robust self-testing is to give a reasonable estimation of how far away the system is from the ideal system when experimental errors or any kind of imperfections are presented in the statistics. If we denote the system that gives an ideal self-testing of some certain state as $|\tilde{\phi}\rangle$, and the system that gives an imperfect statistics as $|\phi\rangle$, the distance of the two can be evaluated as

$$\begin{aligned} D =& \| \Psi(|\phi\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A'B'}}) - \Psi(|\tilde{\phi}\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A'B'}}) \| \\ =& \| \, |\text{junk}\rangle_{\mathcal{AB}} \otimes |\varphi\rangle_{\mathcal{A'B'}} - |\text{junk}\rangle_{\mathcal{AB}} \otimes |\tilde{\varphi}\rangle_{\mathcal{A'B'}} \, \|, \end{aligned} \tag{3.19}$$

where $|\tilde{\varphi}\rangle$ and $|\varphi\rangle$ correspond to the ideal self-testing and imperfect one. However, we can even get rid of the junk and estimate the distance of the ancillary qubits after applying the isometry. We could use the fidelity to measure this distance

$$F = \| \, \langle \tilde{\varphi} | \varphi \rangle_{\mathcal{A'B'}} \, \|^2. \tag{3.20}$$

We use the standard formalism of semidefinite program as in (2.52) and the input of the program, $p(ab|xy)$, is constrained as

$$|p(ab|xy) - \tilde{p}(ab|xy)| \leq \varepsilon, \tag{3.21}$$

where $\tilde{p}(ab|xy)$ is the probability distribution from the ideal system and ε is maximum fluctuation of the probabilities over the ideal ones.

To proceed with the SDP, we first need to define a valid isometry. The control operators defined in (3.13) are good candidates for the isometry. However, the unitarity of these operators holds only if the statistics are ideal, and such properties will disappear once there are errors in the statistics. Due to the fact that, the way the errors appear may have no specific patterns, it is also impossible to define a set of operators that are strictly unitary. The way to solve this problem is to introduce a new unitary operator called ”localizing matrix” [56, 65] that has the same eigenvalues as the one defined in (3.13). For instance, we could define $X'_A = A_2$ which is unitary and simply set the constraint

$$A_2 X_A = A_2(A_1 - \cos(\alpha_{00} + \alpha_{10})A_0)/\sin(\alpha_{00} + \alpha_{10}) \geq 0, \tag{3.22}$$

which will assure A_2 and X_A to share the same eigenvalues. After this tweak, we can simply use X'_A as a valid control operator. We can also do the same trick to Z_B and X_B and then define the isometry we want. However, before we proceed, there is still something which we can do to simplify the problem. If we apply a rotation of $R_y(\alpha_{00}) = \exp(-i\sigma_y\alpha_{00}/2)$ on the subsystem of B, the target state will become

$$|\tilde{\varphi}\rangle = \cos(\frac{\alpha_{00}}{2})\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \sin(\frac{\alpha_{00}}{2})\frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{3.23}$$

and the ideal control operators will become

$$\begin{aligned}
Z_A &= A_0, \\
X_A &= \frac{A_1 - \cos(\alpha_{00} + \alpha_{10})A_0}{\sin(\alpha_{00} + \alpha_{10})}, \\
Z_B &= B_0, \\
X_B &= \frac{B_1 - \cos(\alpha_{10} + \alpha_{11})B_0}{\sin(\alpha_{11} + \alpha_{10})}.
\end{aligned} \tag{3.24}$$

Now, we only need to construct the localizing matrices A_2 and B_2 for X_A and X_B.

The SDP will become

$$\begin{aligned}
\min \quad & F(S) \\
\text{such that} \quad & |\langle\phi|\,\Pi_{a|x}\Pi_{b|y}\,|\phi\rangle_{\mathcal{AB}} - \tilde{p}(ab|xy)| \leq \varepsilon, \\
& \Gamma(S) \geq 0, \\
& \Gamma_{S_A}(A_2X_A) \geq 0, \\
& \Gamma_{S_B}(B_2X_B) \geq 0,
\end{aligned} \tag{3.25}$$

where S_A is a set subset of S and $\Gamma_{S_A}(A_2X_A)_{s,t} = \langle\phi|\, s^\dagger A_2X_At\,|\phi\rangle$ for $s,t \in S_A$. As we have discussed already, we do not have the computational power for $S = S_\infty$, so normally we use S_n for certain n as a relaxation of the SDP. In this case, it turns out to be that S_3 is enough to give a good bound even after we remove some elements in S_3. The S we are using here is

$$S = \{\mathbb{1}, A_x, B_y, A_xB_y, A_xA_{x'}, B_yB_{y'}, A_0A_{1/2}A_0, B_0B_{1/2}B_0\}, \tag{3.26}$$

and the sequence for $\Gamma_{S_A}(A_2X_A)$ and $\Gamma_{S_B}(B_2X_B)$ are

$$\begin{aligned}
S_A &= \{\mathbb{1}, A_0, A_1, A_2\}, \\
S_B &= \{\mathbb{1}, B_0, B_1, B_2\}.
\end{aligned} \tag{3.27}$$

In Figure 3.4, we present the robustness bounds for different setting of measurements. Since there are too many choices of measurement settings, we only plot a few cases that cover both CHSH and the reduced Mayers-Yao, which have the settings $\alpha_{00} = \pi/4$ and $\alpha_{10} = \pi/4$ with the rest two angle being freely changing. For comparison, we also include the robustness bound of the original Mayers-Yao in the plot. It seems that the CHSH will always have the best performance in terms of robustness and the reduced Mayers-Yao performs worse than the original Mayers-Yao. However, the comparison is not conclusive since all the robustness bounds are not tight anyway.

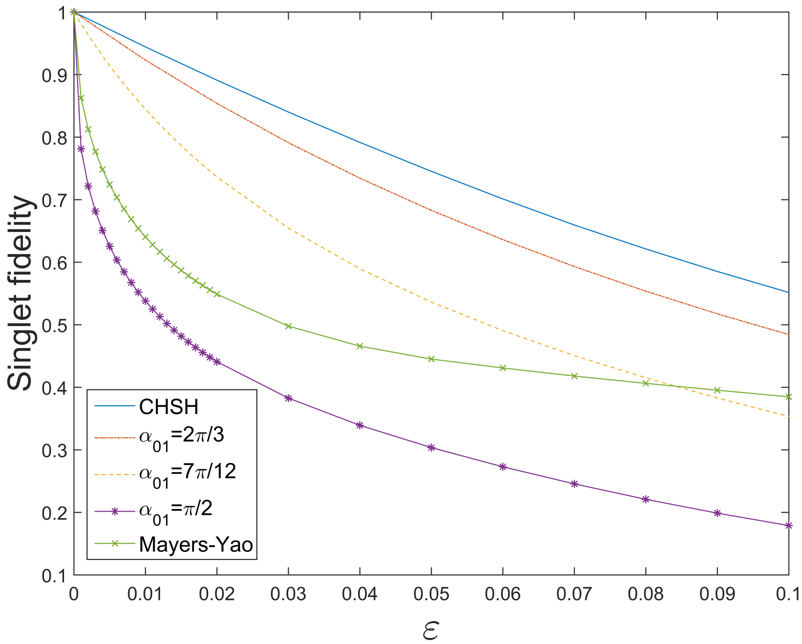


Figure 3.4: Robustness bound for the singlet fidelity F as a function of the imperfections of the observed correlations ε. We plot the bounds for four four-setting criteria ($\theta = \pi/2, \alpha_{00} = \pi/4, \alpha_{01}$) and for the five-setting MayersYao criterion.

3.2.3 The inequalities

A nice feature of self-testing is that only boundary points of the quantum set could be self-tested. Hence whenever a self-testing is achieved, a point at the quantum boundary will be identified. As a result of all the self-testing of singlet states, it confirms the result by [2, 69, 70, 72] that the equality (3.2) defines all the extremal points of the quantum boundary for the (2,2,2) scenario in the slice of zero marginals ($\sum_y E_{xy} = \sum_y E_{xy} = 0$). Since we have the boundary in this slice parametrized, it could be possible to derive the inequality that is maximally violated by each extremal point in this slice.

Let us consider the subspace E with the basis $(\vec{e}_{00}, \vec{e}_{01}, \vec{e}_{10}, \vec{e}_{11})$. The parametrization of the quantum boundary is

$$\begin{aligned} E_{00} &= \cos(\alpha_{00}), \\ E_{01} &= \cos(\alpha_{00}+\alpha_{10}+\alpha_{11}), \\ E_{10} &= \cos(\alpha_{10}), \\ E_{11} &= \cos(\alpha_{11}). \end{aligned} \tag{3.28}$$

A generalization of the cross product in the high dimension space will give the normal vector. At each point in this subspace, there are three vectors that could be defined to be tangent to the boundary, which are

$$\begin{aligned} \vec{v}_1 &= \frac{\partial E}{\partial \alpha_{00}} = \big(-\sin(\alpha_{00}), -\sin(\alpha_{00}+\alpha_{10}+\alpha_{11}), 0, 0\big), \\ \vec{v}_2 &= \frac{\partial E}{\partial \alpha_{10}} = \big(0, -\sin(\alpha_{00}+\alpha_{10}+\alpha_{11}), -\sin(\alpha_{10}), 0\big), \\ \vec{v}_3 &= \frac{\partial E}{\partial \alpha_{11}} = \big(0, -\sin(\alpha_{00}+\alpha_{10}+\alpha_{11}), 0, -\sin(\alpha_{11})\big), \end{aligned} \tag{3.29}$$

and the normal vector would be the cross product

$$\begin{aligned} \vec{n} = \bigwedge(\vec{v}_1, \vec{v}_2, \vec{v}_3) &= \begin{vmatrix} v_1^1 & v_1^2 & v_1^3 & v_1^4 \\ v_2^1 & v_2^2 & v_2^3 & v_2^4 \\ v_3^1 & v_3^2 & v_3^3 & v_3^4 \\ \vec{e}_{00} & \vec{e}_{01} & \vec{e}_{10} & \vec{e}_{11} \end{vmatrix} \\ &= \big(\sin^{-1}(\alpha_{00}), -\sin^{-1}(\alpha_{00}+\alpha_{10}+\alpha_{11}), \sin^{-1}(\alpha_{10}), \sin^{-1}(\alpha_{11})\big). \end{aligned} \tag{3.30}$$

Hence, the inequality of at each point which defines the quantum boundary will be

$$\begin{aligned} \mathcal{I} = \vec{n}\cdot\vec{E} &= \frac{E_{00}}{\sin(\alpha_{00})} - \frac{E_{01}}{\sin(\alpha_{00}+\alpha_{10}+\alpha_{11})} + \frac{E_{10}}{\sin(\alpha_{10})} + \frac{E_{11}}{\sin(\alpha_{11})} \\ &\leq \cot(\alpha_{00}) - \cot(\alpha_{00}+\alpha_{10}+\alpha_{11}) + \cos(\alpha_{10}) + \cos(\alpha_{11}), \end{aligned} \tag{3.31}$$

where the maximal is achieved with the corresponding boundary point (3.28). This also recovers the game which is defined in the work by Miller and Shi [73]. We could notice that the inequality coincides with the CHSH inequality when $\alpha_{00} = \alpha_{10} = \alpha_{11} = \pi/4$.

Since we are confined in a specific slice, generally speaking, it is not confirmed whether theses inequalities are the ones that are maximally violated in the full correlation space $\mathcal{C}$, which is equivalent to the probability space $\mathcal{P}$ here. However, because these points self-test the singlet state within the whole space $\mathcal{C}$, there must exist an inequality for each of them in $\mathcal{C}$. As seen from the above result, the inequality we derived from the four dimensional space is unique for each point, so we confirm that these inequalities are actually the inequalities which characterize the extremal point in the whole correlation space.

A sketch that shows the slice we studied with all the marginal statistics to be zero could be found in Figure 3.5. In fact, one could see that the inequalities (3.31) we found above are actually the tangent planes of boundary points of the quantum set $\mathcal{Q}$ in Figure 3.5.

3.3 α-inequality and self-testing of partially entangled qubit state

As we have shown in the previous section, the maximally entangled state could be self-tested. Now the question arises that whether we can self-test any bipartite qubit state. Of course, we only consider pure state for self-testing. It turns out that we are able to do that as long as the state is entangled.

This result was first shown in the work of [54], and later a flaw in the proof was corrected in [74] while confirming the inequality-based criterion. It used a tilted CHSH inequality called α-inequality which is maximally violated by the partially entangled state to achieve the self-testing. This could be summarized as the following theorem.

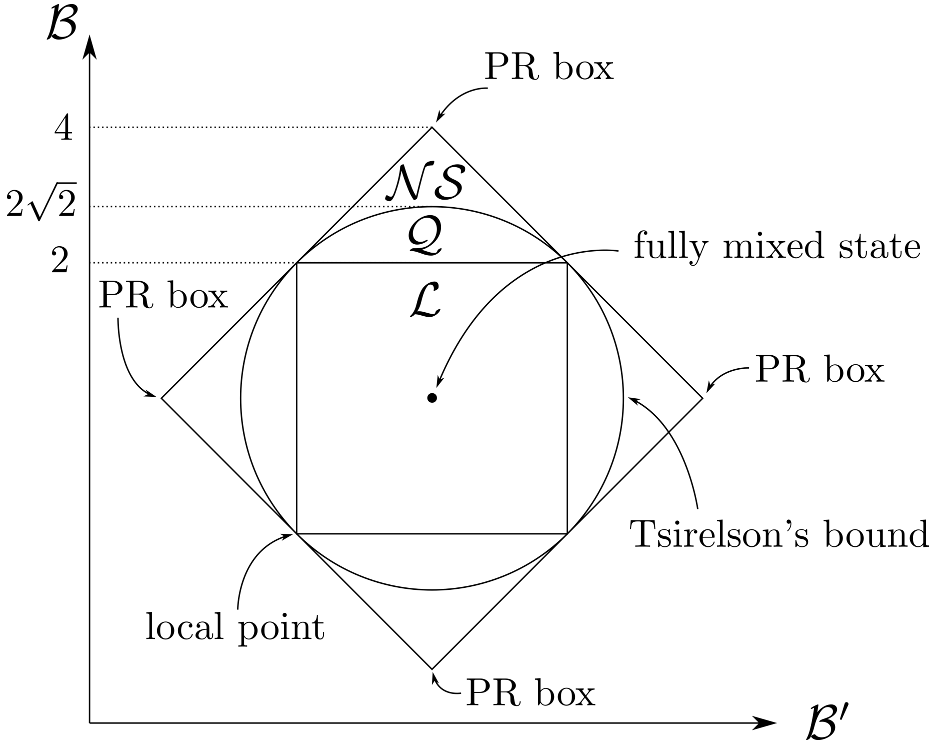


Figure 3.5: Slice in the space $\mathcal{C}$ of the (2,2,2) scenario where marginal statistics are all zero. $\mathcal{B}$ is the CHSH inequality and $\mathcal{B}'$ is also a CHSH inequality but with relabelled indexes of inputs and outputs. The Tsirelson's bound, which is maximally violated using singlet state, is also recovered by the equality (3.2).

Theorem 9. *In the (2,2,2) scenario, if the α-inequality*

$$\mathcal{I}_\alpha = \alpha E_{0\times} + E_{00} + E_{01} + E_{10} - E_{11} \leq \sqrt{8 + 2\alpha^2}, \tag{3.32}$$

is violated maximally for $\alpha \in [0, 2]$ [75], where $E_{i\times}$ stands for the probability marginal on A and same for B with $E_{\times j}$, then there exists a local isometry $\Psi = \Psi_A \otimes \Psi_B$, such that for the state of the device $|\phi\rangle$ and the measurements A_i, B_j ($i, j \in \{0, 1\}$):

$$\Psi(|\phi\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A}'\mathcal{B}'}) = |junk\rangle_{\mathcal{AB}} \otimes |\theta\rangle_{\mathcal{A}'\mathcal{B}'}\,, \tag{3.33}$$

$$\Psi(A_iB_j\,|\phi\rangle_{\mathcal{AB}} \otimes |00\rangle_{\mathcal{A}'\mathcal{B}'}) = |junk\rangle_{\mathcal{AB}} \otimes (\sigma_i \otimes \sigma_j)\,|\theta\rangle_{\mathcal{A}'\mathcal{B}'}\,, \tag{3.34}$$

where σ-s are linear combinations of the Pauli operations on the ancillary qubits, $|\theta\rangle = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle$ for $\theta \in (0, \pi/2)$ and $\sin(2\theta) = \sqrt{(1-\alpha^2)/(1+\alpha^2)}$

The proof of the self-testing could also be found in [54]. It was originally proved analytically using the technique of Sum of Square (SOS) [54, 74]. In the next section, we will cover the SDP method of the self-testing in this case. Hence, we are not going to discuss in detail about the proof here.

It is important to point out that the reason why only the state $|\theta\rangle$ is considered is due to the fact that, any pure entangled state could always be written in the form of $|\theta\rangle$ in certain basis.

Since the criterion of the inequality being maximally violated is equivalent to the full probability distribution given the optimal strategy that achieve the maximal violation, one could still have the self-testing if the probability distribution is provided. In this case, the optimal strategy is given by the state $|\theta\rangle$ measured by

$$\begin{aligned} A_0 &= \sigma_x, & A_1 &= \sigma_x, \\ B_0 &= \cos(\mu)\sigma_z - \sin(\mu)\sigma_x, & B_1 &= \cos(\mu)\sigma_z + \sin(\mu)\sigma_x, \end{aligned} \tag{3.35}$$

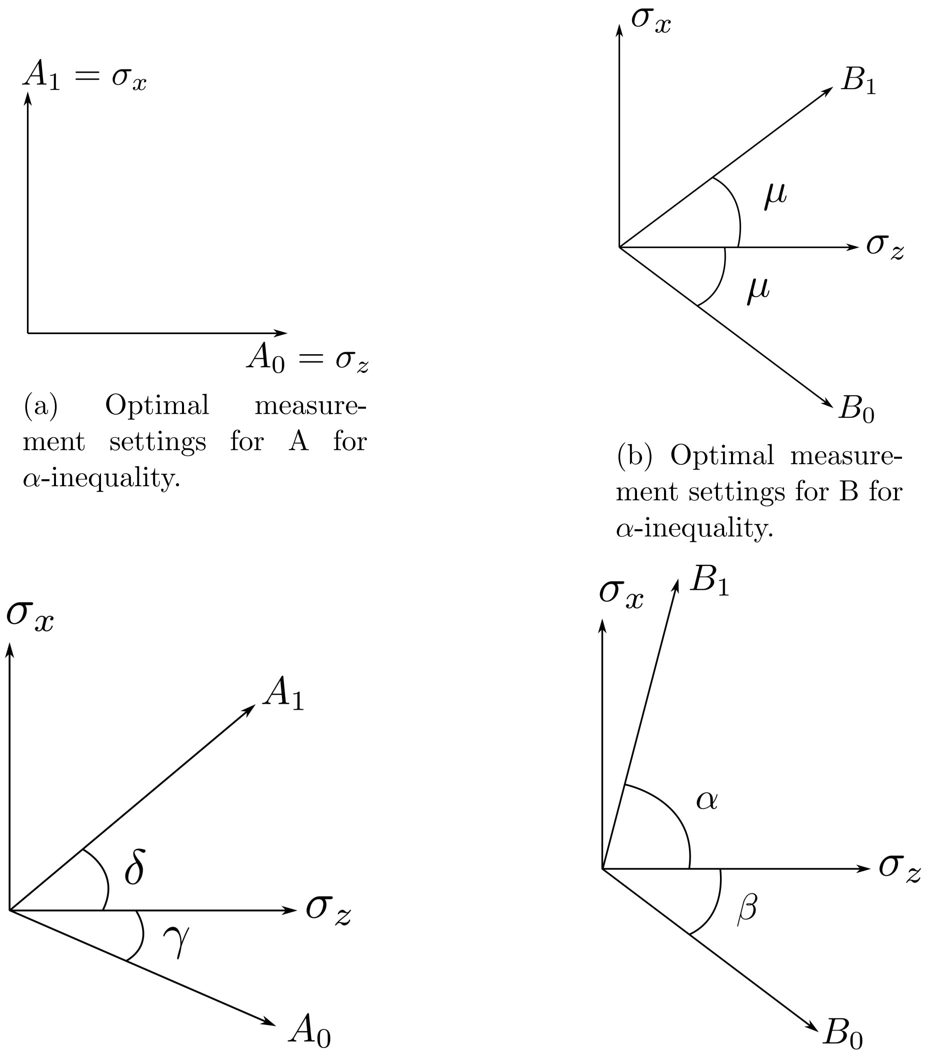
where $\tan(\mu) = \sin(2\theta)$.

3.4 All the extremal points that self-test the partially entangled state

In section 3.2, we have shown that the singlet state actually has a whole set of different self-testings. This intrigues us to think whether this is also the case for the partially entangled states. However, to get an analytical proof of more self-testings of the partially entangled state, it would require a lot more computations. On the other hand, self-testing with SDP provides us a new way to tackle the problem. Since it does not have that much of mathematical proofs compared to the analytical method, it is faster and simpler to find out whether the proposed self-testing is working or not by SDP. In this section, we will basically use the SDP method, and show that all the extremal points in the (2,2,2) scenario (see Section 3.4.3), except for the local deterministic points, will self-test the partially entangled state.

3.4.1 The self-testings

From Chapter 2, we see that for qubit system, the key to define a valid isometry is to find a pair of anti-commutative operators on each party. In the case of the singlet state, we manage to vary the measurement directions from the ideal CHSH ones arbitrarily up to condition (3.2) and still prove the anti-commutativity of the operators defined as (3.13). Hence, we are also willing to see whether it still gives us a self-testing by changing the direction of the measurements arbitrarily up to some constraints.



(a) Optimal measurement settings for A for α-inequality.

(b) Optimal measurement settings for B for α-inequality.

(c) Measurement settings for A in the arbitrary case.

(d) Measurement settings for B in the arbitrary case.

Figure 3.6: Measurement settings for the partially entangled state.

As in Figure 3.6, we have sketched out the ideal measurements to self-test with the α-inequality self-testing and the measurements in arbitrary directions.

The corresponding new measurements are

$$\begin{aligned} A_0 &= \cos(\gamma)\sigma_z - \sin(\gamma)\sigma_x, & A_1 &= \cos(\delta)\sigma_z + \sin(\delta)\sigma_x, \\ B_0 &= \cos(\beta)\sigma_z - \sin(\beta)\sigma_x, & B_1 &= \cos(\alpha)\sigma_z + \sin(\alpha)\sigma_x. \end{aligned} \tag{3.36}$$

The task for us is to see if one has the statistics from the state $|\theta\rangle$ measured by these operators, will it give us a self-testing regarding some certain configurations $(\alpha, \beta, \gamma, \delta)$?

In a formal way, the question could be stated as, if we observed the statistics

$$\begin{aligned} E_{0\times} &= \cos(2\theta)\cos(\gamma) \qquad E_{1\times} = \cos(2\theta)\cos(\delta) \\ E_{\times 0} &= \cos(2\theta)\cos(\beta) \qquad E_{\times 1} = \cos(2\theta)\cos(\alpha) \\ E_{00} &= \cos(\beta)\cos(\gamma) + \sin(2\theta)\sin(\beta)\sin(\gamma) \\ E_{01} &= \cos(\alpha)\cos(\gamma) - \sin(2\theta)\sin(\alpha)\sin(\gamma) \\ E_{10} &= \cos(\beta)\cos(\delta) - \sin(2\theta)\sin(\beta)\sin(\delta) \\ E_{11} &= \cos(\alpha)\cos(\delta) + \sin(2\theta)\sin(\alpha)\sin(\delta) \end{aligned} \tag{3.37}$$

can we show a self-testing of state $|\theta\rangle$?

The good feature about self-testing with SDP is that one does not have to go through all the mathematics to prove the rigidity of the ideal self-testing. The only thing needed is to define a valid isometry and plug into the SDP program with the statistics and let it run. As long as the SDP output a fidelity of one regarding the target state, we may conclude the self-testing of the state.

To define a valid isometry, we may get some inspirations from the 'believed' optimal strategy as the measurements in (3.36) have already shed light on the possible control operators. Before we write down the control operators, we will also play the same trick as in (3.23) and (3.24). After a rotation of $R_y(\gamma)$ on the first qubit and a rotation of $R_y(\beta)$ on the second qubit, the original target state $|\theta\rangle$ will be transformed into

$$\begin{aligned}|\tilde{\theta}\rangle =&\cos(\frac{\gamma}{2})\cos(\frac{\beta}{2})\,|\theta\rangle + \sin(\frac{\gamma}{2})\sin(\frac{\beta}{2})\,|\theta_1\rangle \\ &+ \cos(\frac{\gamma}{2})\sin(\frac{\beta}{2})\,|\theta_2\rangle + \sin(\frac{\gamma}{2})\cos(\frac{\beta}{2})\,|\theta_3\rangle\,,\end{aligned} \tag{3.38}$$

where $|\theta_1\rangle = \sin(\theta)\,|00\rangle + \cos(\theta)\,|11\rangle$, $|\theta_2\rangle = \cos(\theta)\,|01\rangle - \sin(\theta)\,|10\rangle$ and $|\theta_3\rangle = -\sin(\theta)\,|01\rangle + \cos(\theta)\,|10\rangle$. The corresponding optimal measurements will become

$$\begin{aligned}\tilde{A}_0 &= \sigma_z, & \tilde{A}_1 &= \cos(\gamma+\delta)\sigma_z + \sin(\gamma+\delta)\sigma_x, \\ \tilde{B}_0 &= \sigma_z, & \tilde{B}_1 &= \cos(\alpha+\beta)\sigma_z + \sin(\alpha+\beta)\sigma_x.\end{aligned} \tag{3.39}$$

Now with the clean form above, we can simply write down the control operators

$$\begin{aligned}Z_A &= \tilde{A}_0, \\ X_A &= \frac{\tilde{A}_1 - \cos(\gamma+\delta)\tilde{A}_0}{\sin(\gamma+\delta)}, \\ Z_B &= \tilde{B}_0, \\ X_B &= \frac{\tilde{B}_1 - \cos(\alpha+\beta)\tilde{B}_0}{\sin(\alpha+\beta)}.\end{aligned} \tag{3.40}$$

However, since we do not know if such a setting will give us a self-testing even if the statistics are perfectly matching (3.37), we cannot assure the unitarity of the operators defined above. To solve this problem, again, as for the singlet case, we introduce two localizing matrices, A_2 and B_2, and impose the constraints that

$$\begin{aligned}A_2 X_A &\geq 0, \\ B_2 X_B &\geq 0.\end{aligned} \tag{3.41}$$

Now we can finalize the formalization of the semidefinite program as

$$\begin{aligned}\text{min} \quad & F(S) \\ \text{such that} \quad & \langle\phi|\,\Pi_{a|x}\Pi_{b|y}\,|\phi\rangle_{\mathcal{AB}} = p(ab|xy), \\ & \Gamma(S) \geq 0, \\ & \Gamma_{S_A}(A_2X_A) \geq 0, \\ & \Gamma_{S_B}(B_2X_B) \geq 0,\end{aligned} \tag{3.42}$$

where $p(ab|xy)$ is the probability distribution from (3.37). For the sequence S, S_A and S_B, we keep them the same as what we have used in the singlet case as (3.26) and (3.27).

We list below the minimum of the fidelity for a few cases with different $(\alpha, \beta, \gamma, \delta, \theta)$.

	α	β	γ	δ	θ	F_{min}
	45°	0	0	120°	35°	0.998244154919248
	19°	25°	5°	95°	25°	0.999999654068137
	35°	25°	5°	100°	15°	0.999994305252953
	14°	0	0	115°	5°	0.999034127029206
Hardy	68.5414°	35.1132°	68.5414°	35.1132°	24.9060°	0.999103351320114

Table 3.1: List of fidelity from SDP with different $(\alpha, \beta, \gamma, \delta, \theta)$.

In the table, we also list the point that represents the Hardy paradox [76] (in a rotated basis) for example, which is the state

$$|\varphi\rangle = \sqrt{(1-a^2)/2}\,|01\rangle + \sqrt{(1-a^2)/2}\,|10\rangle + a\,|11\rangle\,, \tag{3.43}$$

measured by

$$\begin{aligned} A_0 &= \sigma_z, & A_1 &= \cos(\eta)\sigma_z + \sin(\eta)\sigma_x, \\ B_0 &= \sigma_z, & B_1 &= \cos(\eta)\sigma_z + \sin(\eta)\sigma_x, \end{aligned} \tag{3.44}$$

where $a = \sqrt{\sqrt{5}-2}$ and $\cos(\eta) = a^2$.

As the results shown, there is indeed a big part in the space of $(\alpha, \beta, \gamma, \delta, \theta)$ can be self-tested. As we will see later in Section 3.4.3, those points which can be self-tested definitely include all the extremal points of th quantum set. The Hardy point actually behaves differently than the other extremal points in this set. We will cover more detail about this in Section 3.4.2.

The measurement settings (3.36) and state $|\theta\rangle$ which deliver self-testings actually cover all the extremal points that could self-test the partially entangled qubit state in the (2,2,2) scenario. The reason could be found in Section 3.4.3.

As for the robustness of these self-testings, it is for sure that one could get some bound following the same method as what we did in the singlet case. However, since the main concern here is the existence of self-testing, we will not discuss the robustness further.

3.4.2 The inequalities

We know from Chapter 2 that for any SDP program that gives a self-testing of a quantum state, the dual problem of the primal will give the inequality that is maximally violated by the state. It is also not exceptional here, the dual problem will definitely give the inequality that is maximally violated by the partially entangled state $|\theta\rangle$.

Although in the previous section we have shown the self-testing with the α-inequality, it is not a bad idea to retrieve the inequality again using the dual of the SDP program to check the consistency. Specifically, we consider the case when $\alpha = 1$ in Theorem 9. The α-inequality will simply be

$$\mathcal{I}_1 = E_{0\times} + E_{00} + E_{01} + E_{10} - E_{11}. \tag{3.45}$$

What is interesting is that, the inequality we derived from the dual of the SDP is

$$\begin{aligned}\mathcal{I}_1' = &-0.30805177E_{0\times} + 0.016737746E_{1\times} - 0.24839279E_{\times 0} - 0.28919283E_{1\times} \\ &- 0.55811724E_{00} - 0.5610094E_{01}0.72157791E_{10} - 0.73465683E_{11},\end{aligned} \tag{3.46}$$

and it is surprisingly not the same as the α-inequality. This leads us to have the idea that the inequality from the dual program may be wrong. To test if the inequality is legitimate, it is not difficult to check the maximal violation of the inequality by a simple semidefinite program

$$\begin{aligned} \min \quad & -\mathcal{I}_1'(S) \\ \text{such that} \quad & \Gamma(S) \geq 0. \end{aligned} \tag{3.47}$$

From the result of the SDP, the maximal violation of the $\mathcal{I}_1'$ is

$$\max_{SDP} \mathcal{I}_1' = 2.039276242265367. \tag{3.48}$$

We could also just input the statistics given by the optimal strategy and get the value of the α-inequality

$$\mathcal{I}_1'(\text{optimal}) = 2.039121937171557. \tag{3.49}$$

The relative difference of this two value is

$$\begin{aligned} \frac{\max_{SDP} \mathcal{I}_1' - \mathcal{I}_1'(\text{optimal})}{\mathcal{I}_1'(\text{optimal})} &= \frac{2.039276242265367 - 2.039121937171557}{2.039121937171557} \\ &= 7.567232297229453 \times 10^{-5}, \end{aligned} \tag{3.50}$$

which is quite reasonable to make us believe that actually $\mathcal{I}_1'$ is the inequality that is maximally violated by the state in Theorem 9 and also self-tests the state.

The above result is quite interesting because it basically tells us that for a specific boundary point of the quantum set $\mathcal{Q}$, there may exit not only one inequality that characterizes it. Following this intuition, we are looking forward to seeing the different inequalities that characterize the same boundary point.

From Section 3.2.3, we see that if there is a parametrized representation of the boundary of the quantum set, we can actually derive the inequality that characterizes each boundary point in the correlation space. However, if we take a look at the correlations (3.37), we find that there are actually only five free parameters for the eight correlations including the marginals. Hence, it is not possible to define an unique inequality that specifies each point in the eight dimensional space $\mathcal{C}$. This might be the reason that why there are two inequalities that both characterize the point for $\alpha = 1$ in Theorem 9. Since we know that in the space $\mathcal{C}$, $\mathcal{Q}$ is a eight-dimension set, hence, the boundary of $\mathcal{Q}$ must be a seven-dimension hypersurface. A possible explanation could be that, in fact, the boundary points of the quantum set that we have found are not part of a seven-dimension hypersurface within a local region. Within this region, the boundary of the quantum set is just a five-dimension hypersurface. One could imagine the rim of on side of a curved surface as an example (the green line in Figure 3.7). The purple plane, which represents the inequality that is maximally violated by the extremal point, contacts with the quantum set at a point which has a lower dimension than the whole quantum set. This is also the reason why we will see later that this plane which defines the inequality could actually rotate freely to some extent.

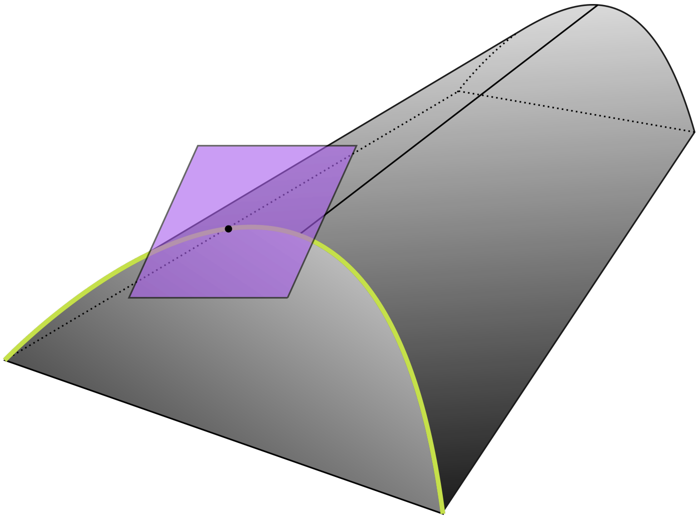


Figure 3.7: A conceptual sketch of how the quantum set may look like.

As we have mentioned, even though the set of points we derived here do not form a seven-dimension hypersurface on the quantum boundary, it is still possible to get some non-trivial inequalities that are maximally violated by those points. To define an inequality, it is the same to state the normal vector of the hyperplane define by the inequality. For a specific point

$$c = c(E_{0\times}, E_{1\times}, E_{\times 0}, E_{\times 1}, E_{00}, E_{01}, E_{10}, E_{11}), \tag{3.51}$$

in $\mathcal{C}$, let us denote the inequality belongs to it with $\vec{n}$. From the parametrized boundary points we found, we could at most derive five tangent vectors at each point, which are

$$\vec{v}_1 = \frac{\partial c}{\partial \alpha},\ \vec{v}_2 = \frac{\partial c}{\partial \beta},\ \vec{v}_3 = \frac{\partial c}{\partial \gamma},\ \vec{v}_4 = \frac{\partial c}{\partial \delta},\ \vec{v}_5 = \frac{\partial c}{\partial \theta}. \tag{3.52}$$

These vectors are all orthogonal to $\vec{n}$,

$$\vec{n} \cdot \vec{v}_1 = 0,\ \vec{n} \cdot \vec{v}_2 = 0,\ \vec{n} \cdot \vec{v}_3 = 0,\ \vec{n} \cdot \vec{v}_4 = 0,\ \vec{n} \cdot \vec{v}_5 = 0. \tag{3.53}$$

To these point, we manage to fix five out of the eight degrees of freedom of $\vec{n}$, and there is nothing we can do to fix the other three. Hence, what we can do is to manually assign the three degrees some certain values. However, this inequality defined by $\vec{n}$ may not be promised to characterize the point c, since it could happen that $\vec{n}$ is pointing at some other parts of the quantum set. On the other hand, the vectors that is near a known valid vector $\vec{n}^*$ will be highly probably define a valid inequality. Hence, we could do our numerical search around $\vec{n}^*$, which means

$$\vec{n} \cdot \vec{n}^* \geq 1 - \varepsilon, \tag{3.54}$$

where ε is a constant and supposed to be very small compared to 1. One more thing should be paid attention to is that whether $\vec{n}$ is an outward or inward vector. Once we found that the inequality define by $\vec{n}$ is not maximally violated by c, we could just invert the vector and check the maximal violation again.

With the method described above, we manage to find more inequalities that define the points in the α-inequality self-testing, such as

$$\begin{aligned}\mathcal{I}_1'' = &-0.30805177E_{0\times} + 0.016737746E_{1\times} - 0.24839279E_{\times 0} - 0.28919283E_{1\times} \\ &- 0.55811724E_{00} - 0.5610094E_{01}0.72157791E_{10} - 0.73465683E_{11},\end{aligned} \tag{3.55}$$

$$\begin{aligned}\mathcal{I}_1'' = &-0.30805177E_{0\times} + 0.016737746E_{1\times} - 0.24839279E_{\times 0} - 0.28919283E_{1\times} \\ &- 0.55811724E_{00} - 0.5610094E_{01}0.72157791E_{10} - 0.73465683E_{11}.\end{aligned} \tag{3.56}$$

For the Hardy point, first of all, we could derive the inequality from the dual of the SDP program

$$\begin{aligned}\mathcal{I}_{Hardy} = &-0.002787601707553E_{0\times} - 0.750567748544415E_{1\times} \\ &- 0.776102171961274E_{\times 0} - 0.028370726495952E_{1\times} \\ &+ 0.776919397995680E_{00} - 0.779707763464578E_{01} \\ &+ 0.000810022525836E_{10} + 0.751407698482343E_{11},\end{aligned} \tag{3.57}$$

however, once we follow the method described above, no matter how we lower the value of ε in (3.54), we still cannot find a valid inequality that is maximally violated by the Hardy point. Another strange result we found from the SDP is that, the point that maximizes the $\mathcal{I}_{Hardy}$ is actually not unique, for instance, both the two points bellow

$$\begin{aligned}c_0 =&\big(2-\sqrt{5}, 2\sqrt{5}-5, 2\sqrt{5}-5, 2-\sqrt{5}, \\ &3(\sqrt{5}-2), 2\sqrt{5}-5, 6\sqrt{5}-13, 3(\sqrt{5}-2)\big),\end{aligned} \tag{3.58}$$

$$\begin{aligned}c_1 =&(-0.139728324364676, -0.565721523778005, -0.493599330702860, \\ &-0.328988174023790, 0.646128872869022, -0.531283418205931, \\ &0.416842121534432, 0.763266511249520),\end{aligned} \tag{3.59}$$

could violate $\mathcal{I}_{Hardy}$ maximally to

$$\max_{SDP} \mathcal{I}_{Hardy} = 2.307515 \pm 0.000002. \tag{3.60}$$

This suggest that, any mixture of these two points in between them

$$c_{Hardy} = \lambda c_0 + (1-\lambda)c_1, \qquad 0 \leq \lambda \leq 1, \tag{3.61}$$

will also violate the inequality $\mathcal{I}_{Hardy}$ maximally.

3.4.3 The extremal points and the quantum set of (2,2,2)

We have shown that the state $|\theta\rangle$ together with measurement settings (3.36) define a whole set of criterion that self-test the partially entangled state. There are some consequences following this result.

First, with such a set of self-testings, we could argue that actually it contains all the extremal points of the quantum set in the (2,2,2) scenario, except for some special cases which can be identified. We know from the work of Masanas [71] that in the (2,2,2) scenario, all the extremal points could be achieved with pure entangled qubit states and projective measurements. In addition, any pure entangled qubit bipartite state could be Schmidt decomposed into the form of $|\theta\rangle$, and all the projective measurements considered in (3.36) are free to change into any direction, it is confident to say that the extremal points must be included by the correlations from $|\theta\rangle$ and measurement settings (3.36).

Since we know that only the points on the boundary of the quantum set could be self-tested, the set of self-testings we derived must be on the boundary. Basically, this set is composed of either extremal points or the boundary points in the flat region. If the correlations obtained by $|\theta\rangle$ and measurement settings (3.36) that cannot be self-tested could be excluded from the boundary of the quantum set, then we are safe to say this set contains all the extremal points. With the following argument, it could be confirmed that those correlations could actually be excluded from being extremal points of the quantum set.

Suppose there is a correlation point c in the space of $\mathcal{C}$ which is derived from state $|\theta\rangle$ and measurements (3.36), if it cannot be self-tested and is still an extremal point, there must be at least two different solutions to the equations (3.37). Moreover, these solutions must have different values for θ, since otherwise the state associated to c will be unique and then can be self-tested. Thus, the way to check whether the point c is an extremal point or not is to check whether (3.37) has different solutions with different θs.

We will write down the correlations (3.37) here for convenience,

$$\begin{aligned} E_{0\times} &= \cos(2\theta)\cos(\gamma) \qquad E_{1\times} = \cos(2\theta)\cos(\delta) \\ E_{\times 0} &= \cos(2\theta)\cos(\beta) \qquad E_{\times 1} = \cos(2\theta)\cos(\alpha) \\ E_{00} &= \cos(\beta)\cos(\gamma) + \sin(2\theta)\sin(\beta)\sin(\gamma) \\ E_{01} &= \cos(\alpha)\cos(\gamma) - \sin(2\theta)\sin(\alpha)\sin(\gamma) \\ E_{10} &= \cos(\beta)\cos(\delta) - \sin(2\theta)\sin(\beta)\sin(\delta) \\ E_{11} &= \cos(\alpha)\cos(\delta) + \sin(2\theta)\sin(\alpha)\sin(\delta) \end{aligned}$$

Imagining there are two solutions for fixed correlations E_{xy}, and they have different $\theta \in (0, \pi/2)$, denoted by θ_1 and θ_2. Due to the first four marginals in (3.37), we know that $(\alpha, \beta, \delta, \gamma)$ corresponding to θ_1 and θ_2 must be different. Let us denote the angles belongs to the two different solutions as $(\alpha_1, \beta_1, \delta_1, \gamma_1, \theta_1)$ and $(\alpha_2, \beta_2, \delta_2, \gamma_2, \theta_2)$. From the first four marginals, we have

$$\begin{aligned} \cos(\gamma_2) &= \frac{\cos(2\theta_1)\cos(\gamma_1)}{\cos(2\theta_2)}, \qquad & \cos(\delta_2) &= \frac{\cos(2\theta_1)\cos(\delta_1)}{\cos(2\theta_2)}, \\ \cos(\beta_2) &= \frac{\cos(2\theta_1)\cos(\beta_1)}{\cos(2\theta_2)}, \qquad & \cos(\alpha_2) &= \frac{\cos(2\theta_1)\cos(\alpha_1)}{\cos(2\theta_2)}. \end{aligned}$$

Substituting these relations to the four correlations, we have

$$\sin(2\theta_2)\sin(\beta_2)\sin(\gamma_2) = \sin(2\theta_1)\sin(\beta_1)\sin(\gamma_1) + \left(1 - \frac{\cos^2(2\theta_1)}{\cos^2(2\theta_2)}\right)\cos(\beta_1)\cos(\gamma_1), \tag{3.62}$$

$$\sin(2\theta_2)\sin(\alpha_2)\sin(\gamma_2) = \sin(2\theta_1)\sin(\alpha_1)\sin(\gamma_1) - \left(1 - \frac{\cos^2(2\theta_1)}{\cos^2(2\theta_2)}\right)\cos(\alpha_1)\cos(\gamma_1), \tag{3.63}$$

$$\sin(2\theta_2)\sin(\beta_2)\sin(\delta_2) = \sin(2\theta_1)\sin(\beta_1)\sin(\delta_1) - \left(1 - \frac{\cos^2(2\theta_1)}{\cos^2(2\theta_2)}\right)\cos(\beta_1)\cos(\delta_1), \tag{3.64}$$

$$\sin(2\theta_2)\sin(\alpha_2)\sin(\delta_2) = \sin(2\theta_1)\sin(\alpha_1)\sin(\delta_1) + \left(1 - \frac{\cos^2(2\theta_1)}{\cos^2(2\theta_2)}\right)\cos(\alpha_1)\cos(\delta_1). \tag{3.65}$$

Obviously, the product of the r.h.s. of (3.62) and (3.65) will be equal to that of the (3.63) and (3.64), since the l.h.s. are equal. After simplification, we get

$$\begin{aligned}\left(1 - \frac{\cos^2(2\theta_1)}{\cos^2(2\theta_2)}\right)\sin(2\theta_1)\Big(&\cos(\alpha_1)\sin(\beta_1)\sin(\gamma_1)\cos(\delta_1)\\ &+\sin(\alpha_1)\cos(\beta_1)\cos(\gamma_1)\sin(\delta_1)\Big)\\ &=\\ -\left(1 - \frac{\cos^2(2\theta_1)}{\cos^2(2\theta_2)}\right)\sin(2\theta_1)\Big(&\cos(\alpha_1)\sin(\beta_1)\cos(\gamma_1)\sin(\delta_1)\\ &+\sin(\alpha_1)\cos(\beta_1)\sin(\gamma_1)\cos(\delta_1)\Big),\end{aligned} \tag{3.66}$$

which will lead to

$$\left(1 - \frac{\cos^2(2\theta_1)}{\cos^2(2\theta_2)}\right)\sin(2\theta_1)\sin(\alpha_1+\beta_1)\sin(\gamma_1+\delta_1) = 0. \tag{3.67}$$

Since $\theta_1 \neq \theta_2$ and $(\alpha, \beta, \delta, \gamma) \in [0, \pi]$, to satisfy this relation, one of the following cases must happen

$$\begin{cases} \alpha_1 + \beta_1 = \pi, & (3.68) \\ \alpha_1 = \beta_1 = 0, & (3.69) \\ \gamma_1 + \delta_1 = \pi, & (3.70) \\ \gamma_1 = \delta_1 = 0. & (3.71) \end{cases}$$

With the same argument, we could also derive the relations of $(\alpha_2, \beta_2, \delta_2, \gamma_2)$. Let us consider the situation where (3.68) happens. With the four marginals in (3.37), we have

$$\begin{aligned} \cos(\alpha) &= -\cos(\beta) = \frac{E_{\times 1}}{\cos(2\theta)}, \\ \cos(\gamma) &= \frac{E_{0\times}}{\cos(2\theta)}, \\ \cos(\delta) &= \frac{E_{1\times}}{\cos(2\theta)}. \end{aligned}$$

If we substitute them into the four correlations in (3.37), we will get four quadratic equations about $\cos^2(2\theta)$

$$\begin{aligned} &\cos^4(2\theta) + (E_{00}^2 - E_{0\times}^2 - E_{\times 0}^2 - 1)\cos^2(2\theta) \\ &\qquad + (E_{0\times}^2 + E_{\times 0}^2 + E_{0\times}^2 E_{\times 0}^2 - 2E_{0\times}E_{\times 0}E_{00}) = 0, \qquad (3.72) \\ &\cos^4(2\theta) + (E_{01}^2 - E_{0\times}^2 - E_{\times 1}^2 - 1)\cos^2(2\theta) \\ &\qquad + (E_{0\times}^2 + E_{\times 1}^2 + E_{0\times}^2 E_{\times 1}^2 - 2E_{0\times}E_{\times 1}E_{01}) = 0, \qquad (3.73) \\ &\cos^4(2\theta) + (E_{10}^2 - E_{1\times}^2 - E_{\times 0}^2 - 1)\cos^2(2\theta) \\ &\qquad + (E_{1\times}^2 + E_{\times 0}^2 + E_{1\times}^2 E_{\times 0}^2 - 2E_{1\times}E_{\times 0}E_{10}) = 0, \qquad (3.74) \\ &\cos^4(2\theta) + (E_{11}^2 - E_{1\times}^2 - E_{\times 1}^2 - 1)\cos^2(2\theta) \\ &\qquad + (E_{1\times}^2 + E_{\times 1}^2 + E_{1\times}^2 E_{\times 1}^2 - 2E_{1\times}E_{\times 1}E_{10}) = 0. \qquad (3.75) \end{aligned}$$

Each of the four equations will give two solutions of $\cos^2(2\theta)$. To make them compatible, we need the coefficients of these four equations to be exactly the same, since the coefficients of $\cos^4(2\theta)$ are all 1. This means

$$\begin{aligned}&(E_{00}^2 - E_{0\times}^2 - E_{\times 0}^2 - 1) = (E_{01}^2 - E_{0\times}^2 - E_{\times 1}^2 - 1)\\ =&(E_{10}^2 - E_{1\times}^2 - E_{\times 0}^2 - 1) = (E_{11}^2 - E_{1\times}^2 - E_{\times 1}^2 - 1),\end{aligned} \tag{3.76}$$

or the sum of the first and the last will be equal to that of the middle two's

$$\begin{aligned}&E_{00}^2 - E_{0\times}^2 - E_{\times 0}^2 + E_{11}^2 - E_{1\times}^2 - E_{\times 1}^2\\ &\qquad =E_{01}^2 - E_{0\times}^2 - E_{\times 1}^2 + E_{10}^2 - E_{1\times}^2 - E_{\times 0}^2,\end{aligned} \tag{3.77}$$

which will be simplified to

$$E_{00}^2 + E_{11}^2 = E_{01}^2 + E_{10}^2. \tag{3.78}$$

Now, we can substitute back the solution of $(\alpha_1, \beta_1, \delta_1, \gamma_1, \theta_1)$, which will lead to

$$\sin(2\theta_1)\sin(2\alpha_1)\sin(\gamma_1 + \delta_1)\cos(\gamma_1 - \delta_1) = 0, \tag{3.79}$$

under the case of (3.68). To satisfy this relation, there are three possibilities

$$\begin{cases}\alpha_1 = 0, & (3.80)\\ \gamma_1 + \delta_1 = \pi, & (3.81)\\ \gamma_1 = \delta_1 = 0, & (3.82)\\ \gamma_1 - \delta_1 = \pm\pi/2. & (3.83)\end{cases}$$

For the case of (3.80), the first term and last term in (3.76) will lead to

$$(1 - \cos^2(2\theta_1))(\cos^2(\gamma_1) - \cos^2(\delta_1) = 0, \tag{3.84}$$

which means

$$\gamma_1 = \delta_1. \tag{3.85}$$

For the case of (3.83), again, the first term and last term in (3.76) will lead to

$$\Bigg(\sin^2(\alpha_1) - \cos^2(\alpha_1)\sin^2(2\theta_1)\Bigg)\cos(2\gamma_1) = 0, \tag{3.86}$$

or

$$\Bigg(\sin^2(\alpha_1) - \cos^2(\alpha_1)\sin^2(2\theta_1)\Bigg)\cos(2\delta_1) = 0, \tag{3.87}$$

which gives

$$\begin{cases} \tan(\alpha_1) = \sin(2\theta_1), & (3.88) \\ \gamma_1 = 3\pi/4, \text{ and } \delta_1 = \pi/4, & (3.89) \\ \delta_1 = 3\pi/4, \text{ and } \gamma_1 = \pi/4. & (3.90) \end{cases}$$

After all these cases being found, we still have one more situation that we excluded from the first beginning, which is when $\theta = 0$ or $\theta = \pi/2$. In this case, the state of the system will be the product state $|00\rangle$ or $|11\rangle$. We will see that the correlation in (3.37) will actually be independent on A and B. This will lead to the local strategy and hence only the deterministic points will be non-trivial in the sense that they cannot be decomposed into any combinations of points in $\mathcal{C}$. These local deterministic points are also part of the extremal points of the quantum set $\mathcal{Q}$.

Now, we can summarize all the possible values of $(\alpha, \beta, \delta, \gamma, \theta)$ which will give two solutions with different θs for (3.37).

As shown in the table, we found that in any of the cases that a correlation point c may have two different solutions for $\theta \in (0, \pi/2)$, there will always be one party of A or B performing the two measurements in the same direction, which obviously leads to classical correlations. These correlations could always be decomposed as linear combinations of the local deterministic points. This will suggest that, except for the 16 local deterministic points, those correlations derived from state $|\theta\rangle$ and measurements (3.36) which cannot self-test must not be extremal points, since if they were, as we have proved above, they only have unique solutions for θ except for the

$\alpha+\beta=\pi$	$\alpha=0,\beta=\pi,\gamma=\delta\neq 0$
	$\alpha=\pi,\beta=0,\gamma=\delta\neq 0$
	$\gamma+\delta=\pi$
	$\gamma=\delta=0$
	$\gamma-\delta=\pm\pi/2,\tan(\alpha)=\pm\sin(2\theta)$
$\alpha=\beta=0$	$\gamma=\delta$
$\alpha-\beta=\pm\pi/2$	$\gamma+\delta=\pi,\tan(\gamma)=\pm\sin(2\theta)$
$\alpha=\beta\neq 0$	$\gamma=0,\delta=\pi$
	$\gamma=\pi,\delta=0$
	$\gamma=0,\delta=0$

Table 3.2: List of cases when (3.37) have two solutions with different θs.

non-extremal points in Table 3.2 and it will lead to the self-testing of the state and contradicts to the results. We can summarize the relation of the points belong to different categories in Figure 3.8.

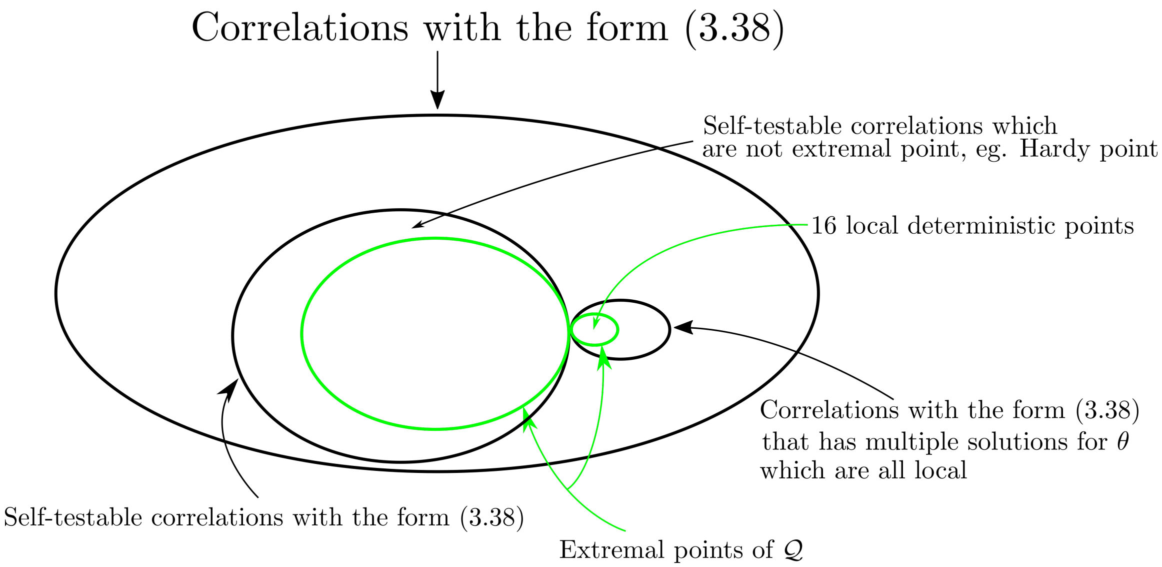

Correlations with the form (3.38)
Self-testable correlations which are not extremal point, eg. Hardy point
16 local deterministic points
Correlations with the form (3.38) that has multiple solutions for θ which are all local
Self-testable correlations with the form (3.38)
Extremal points of $\mathcal{Q}$

Figure 3.8: Different categories of correlations of the form (3.37).

In summary, we manage to show that the set of correlations derived from state $|\theta\rangle$ and measurements (3.36) which can be self-tested actually includes all the extremal points of the (2,2,2) scenario, except for the local deterministic points. Moreover, it also includes some non-extremal points, for instance the flat region we found for Hardy point in the previous section. To this point, in terms of the boundary of the quantum set for the (2,2,2) scenario, what we could say is that, we have all the extremal points already. If there still exists any part of the quantum boundary which is not included in this set we found, they must be flat due to the convexity of the quantum set. Moreover, since these extra flat regions will connect to the extremal part at some point, they must can be expressed as linear combinations of the extremal points we found.

Chapter 4

Self-testing of multipartite systems

Multipartite system is the system which has more than two parties. Compared to bipartite system, it is more difficult to characterize them and the way to study them is also quite different. Multipartite system also has many good properties that make quantum information processing more efficient and useful in many cases than bipartite system, for instance, entanglement distillation [77, 78],quantum error correction [79, 80, 81], fault-tolerant quantum computation and measurement-based quantum computation [82, 83].

In this chapter, we are going to consider the self-testing in the case of multipartite system. More specifically, we are going to start with multipartite qubit states, since it much easier to deal with compared to high dimensional states. Previous study of multipartite system has already shown the self-testing of a large collection of states called graph states [53]. In this chapter, we concentrate more on the non-graph state that could be self-tested.

4.1 Self-testing of 3-qubit W state

4.1.1 The self-testing

Unlike the Greenberger-Horne-Zeilinger (GHZ) state, which belongs to the class of graph state [84, 85] and has been well studied for the purpose of the self-testing in [53], the W state is not in the class and also not studied yet. The n-partite W state take the following form

$$|W_n\rangle = \frac{1}{\sqrt{n}}(|100...0\rangle + |010...0\rangle + ... + |000...1\rangle), \tag{4.1}$$

which is in a superposition of states which has one party being $|1\rangle$ and the rest being $|0\rangle$s. The study of W state becomes interesting since it has the nice property that even if some parties get lost, the state still remains entangled. In this sense, it is more robust against losses. Hence, W state has many applications especially in quantum information processing, for instance superdense coding [86] and information splitting [87]. Thus, the certification of such state becomes interesting both in the sense of real application and for the purpose of self-testing itself.

For simplicity, we will first study the case when $n = 3$, which is the state

$$|W_3\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle). \tag{4.2}$$

A straight observation of this state is that, once we project any of the party into state $|0\rangle$, the state of the rest two parties becomes a maximally entangled state. From the knowledge of Chapter 2, we know that the maximally entangled state could be self-tested. Hence, the above observation lead us to propose the criterion for the self-testing of $|W_3\rangle$ state.

Theorem 10. *A, B and C are spatially separated. A and B each can perform two measurements labelled by $x, y \in \{0.1\}$, C can perform three measurements labelled by $z \in \{0, 1, 2\}$. When measuring on an unknown shared quantum state $|\phi\rangle$, each of them produces binary outcomes labelled by $a, b, c \in \{0, 1\}$. The $|W_3\rangle$ state is self-tested if the following statistics are observed:*

$$\langle\phi| \Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{1|0} |\phi\rangle = \langle\phi| \Pi^A_{0|0}\Pi^B_{1|0}\Pi^C_{0|0} |\phi\rangle = \langle\phi| \Pi^A_{1|0}\Pi^B_{0|0}\Pi^C_{0|0} |\phi\rangle = \frac{1}{3}, \tag{4.3}$$

$$\begin{cases} \langle\phi|\,\Pi^A_{0|0}B_0C_0\,|\phi\rangle = -\langle\phi|\,\Pi^A_{0|0}B_1C_1\,|\phi\rangle = -\dfrac{2}{3}, \\ \langle\phi|\,\Pi^A_{0|0}B_1C_0\,|\phi\rangle = \langle\phi|\,\Pi^A_{0|0}B_0C_1\,|\phi\rangle = 0, \\ \langle\phi|\,\Pi^A_{0|0}B_0C_2\,|\phi\rangle = -\langle\phi|\,\Pi^A_{0|0}B_1C_2\,|\phi\rangle = -\dfrac{\sqrt{2}}{3}, \end{cases} \tag{4.4}$$

$$\begin{cases} \langle\phi|\,\Pi^B_{0|0}A_0C_0\,|\phi\rangle = -\langle\phi|\,\Pi^B_{0|0}A_1C_1\,|\phi\rangle = -\dfrac{2}{3}, \\ \langle\phi|\,\Pi^B_{0|0}A_1C_0\,|\phi\rangle = \langle\phi|\,\Pi^B_{0|0}A_0C_1\,|\phi\rangle = 0, \\ \langle\phi|\,\Pi^B_{0|0}A_0C_2\,|\phi\rangle = -\langle\phi|\,\Pi^B_{0|0}A_1C_2\,|\phi\rangle = -\dfrac{\sqrt{2}}{3}, \end{cases} \tag{4.5}$$

Proof. To begin with the proof, we need to be reminded that all the measurements in self-testing can be treated as projective measurements since the dimension of the Hilbert space is not limited. We can always include those dimensions that make the measurements projective. Moreover, for binary output measurement O which is projective, it is generally true that

$$O^2 = \mathbb{1}. \tag{4.6}$$

These are all the preliminary knowledges we need to know before we entering the proof.

From the observation (4.3), we notice that $\langle\phi|\,\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{1|0}\,|\phi\rangle + \langle\phi|\,\Pi^A_{0|0}\Pi^B_{1|0}\Pi^C_{0|0}\,|\phi\rangle + \langle\phi|\,\Pi^A_{1|0}\Pi^B_{0|0}\Pi^C_{0|0}\,|\phi\rangle = 1$. This hints us that except for the probabilities of the three output combinations above, all the rest are zero

$$\langle\phi|\,\Pi^A_{a|x}\Pi^B_{b|y}\Pi^C_{c|z}\,|\phi\rangle = 0, \qquad a+b+c \neq 1, \tag{4.7}$$

which is also to say

$$\begin{aligned} &\|\Pi^A_{a|x}\Pi^B_{b|y}\Pi^C_{c|z}\,|\phi\rangle\,\| \\ =&\sqrt{\langle\phi|\,\Pi^C_{c|z}\Pi^B_{b|y}\Pi^A_{a|x}\Pi^A_{a|x}\Pi^B_{b|y}\Pi^C_{c|z}\,|\phi\rangle} = 0, \qquad a+b+c \neq 0. \end{aligned} \tag{4.8}$$

It is not a bad idea to carry out the following calculation

$$\begin{aligned}\|\Pi^A_{0|0} B_y \left|\phi\right\rangle \| &= \sqrt{\left\langle\phi\right| B_y^\dagger \Pi^A_{0|0}\Pi^A_{0|0} B_y \left|\phi\right\rangle} = \sqrt{\left\langle\phi\right| \Pi^A_{0|0} \left|\phi\right\rangle} \\ &= \sqrt{\left\langle\phi\right| \Pi^A_{0|0}\Pi^B_{1|0}\Pi^C_{0|0} \left|\phi\right\rangle + \left\langle\phi\right| \Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{1|0} \left|\phi\right\rangle} \\ &= \sqrt{\frac{2}{3}}. \end{aligned} \tag{4.9}$$

For the same reason, we have

$$\|\Pi^A_{0|0} C_z \left|\phi\right\rangle \| = \|\Pi^B_{0|0} A_x \left|\phi\right\rangle \| = \|\Pi^B_{0|0} C_z \left|\phi\right\rangle \| = \sqrt{\frac{2}{3}}. \tag{4.10}$$

From the observation (4.4), we notice that

$$\begin{aligned}\left\langle\phi\right| \Pi^A_{0|0} B_0 C_0 \left|\phi\right\rangle &= \|\Pi^A_{0|0} B_0 \left|\phi\right\rangle \| \cdot \|\Pi^A_{0|0} C_0 \left|\phi\right\rangle \| \cdot \cos(\theta) \\ &= \sqrt{\frac{2}{3}} \cdot \sqrt{\frac{2}{3}} \cdot \cos(\theta) = -\frac{2}{3}, \end{aligned} \tag{4.11}$$

which means the angle between the vectors $\Pi^A_{0|0} B_0 \left|\phi\right\rangle$ and $\Pi^A_{0|0} C_0 \left|\phi\right\rangle$ is

$$\angle(\Pi^A_{0|0} B_0 \left|\phi\right\rangle, \Pi^A_{0|0} C_0 \left|\phi\right\rangle) = \pi. \tag{4.12}$$

Following similar procedure, we could derive the angles for the other vectors

$$\angle(\Pi^A_{0|0} B_1 \left|\phi\right\rangle, \Pi^A_{0|0} C_0 \left|\phi\right\rangle) = \frac{\pi}{2}, \tag{4.13}$$

$$\angle(\Pi^A_{0|0} B_1 \left|\phi\right\rangle, \Pi^A_{0|0} C_1 \left|\phi\right\rangle) = 0, \tag{4.14}$$

$$\angle(\Pi^A_{0|0} B_0 \left|\phi\right\rangle, \Pi^A_{0|0} C_2 \left|\phi\right\rangle) = \frac{3\pi}{4}, \tag{4.15}$$

$$\angle(\Pi^A_{0|0} B_1 \left|\phi\right\rangle, \Pi^A_{0|0} C_2 \left|\phi\right\rangle) = \frac{\pi}{4}. \tag{4.16}$$

With these information, the only possible configuration that these four vectors can be put in the vector space is that they are all in the same plane as in Figure 4.1

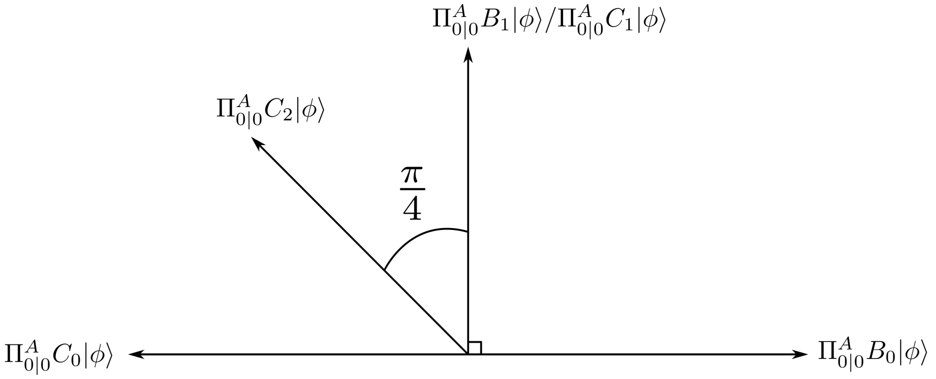

$\Pi^A_{0|0}B_1|\phi\rangle/\Pi^A_{0|0}C_1|\phi\rangle$
$\Pi^A_{0|0}C_2|\phi\rangle$
$\frac{\pi}{4}$
$\Pi^A_{0|0}C_0|\phi\rangle$
$\Pi^A_{0|0}B_0|\phi\rangle$

Figure 4.1: Configuration of vectors in the space for 3-qubit W state.

This implies that

$$\Pi^A_{0|0}C_2\left|\phi\right\rangle = \frac{\Pi^A_{0|0}B_1\left|\phi\right\rangle - \Pi^A_{0|0}B_0\left|\phi\right\rangle}{\sqrt{2}}. \tag{4.17}$$

We could also apply $\Pi^A_{0|0}C_2$ on both sides of the above equation and get

$$\begin{aligned}
&\Pi^A_{0|0}\Pi^A_{0|0}C_2C_2\left|\phi\right\rangle \\
=&\Pi^A_{0|0}\left|\phi\right\rangle = \Pi^A_{0|0}C_2\frac{\Pi^A_{0|0}B_1\left|\phi\right\rangle - \Pi^A_{0|0}B_0\left|\phi\right\rangle}{\sqrt{2}} \\
=&\frac{B_1 - B_0}{\sqrt{2}}\Pi^A_{0|0}C_2\left|\phi\right\rangle = \frac{B_1 - B_0}{\sqrt{2}}\frac{\Pi^A_{0|0}B_1\left|\phi\right\rangle - \Pi^A_{0|0}B_0\left|\phi\right\rangle}{\sqrt{2}} \\
=&\Pi^A_{0|0}(\frac{B_1 - B_0}{\sqrt{2}})^2\left|\phi\right\rangle = \Pi^A_{0|0}\frac{(B_0^2 + B_1^2 - \{B_0, B_1\})}{2}\left|\phi\right\rangle \\
=&\Pi^A_{0|0}\frac{(2\mathbb{1} - \{B_0, B_1\})}{2}\left|\phi\right\rangle = \Pi^A_{0|0}\left|\phi\right\rangle - \Pi^A_{0|0}\frac{\{B_0, B_1\}}{2}\left|\phi\right\rangle.
\end{aligned} \tag{4.18}$$

This will lead to

$$\Pi^A_{0|0}\{B_0, B_1\}\left|\phi\right\rangle = 0, \tag{4.19}$$

which is the anti-commutativity of B_0 and B_1 acting on the system $\left|\phi\right\rangle$ subjective to the projector $\Pi^A_{0|0}$. For the same reason, we can also derive

$$\Pi^B_{0|0}\{A_0, A_1\}\left|\phi\right\rangle = 0. \tag{4.20}$$

From (4.12) and (4.14), we can see that

$$\begin{aligned}\Pi^A_{0|0}B_0 \left|\phi\right\rangle &= -\Pi^A_{0|0}C_0 \left|\phi\right\rangle ,\\ \Pi^A_{0|0}B_1 \left|\phi\right\rangle &= \Pi^A_{0|0}C_1 \left|\phi\right\rangle .\end{aligned}$$

Thus,

$$\begin{aligned}\Pi^A_{0|0}C_0\Pi^A_{0|0}C_1 \left|\phi\right\rangle &= \Pi^A_{0|0}C_0\Pi^A_{0|0}B_1 \left|\phi\right\rangle = \Pi^A_{0|0}B_1\Pi^A_{0|0}C_0 \left|\phi\right\rangle \\ &= -\Pi^A_{0|0}B_1\Pi^A_{0|0}B_0 \left|\phi\right\rangle = \Pi^A_{0|0}B_0\Pi^A_{0|0}B_1 \left|\phi\right\rangle \\ &= \Pi^A_{0|0}B_0\Pi^A_{0|0}C_1 \left|\phi\right\rangle = \Pi^A_{0|0}C_1\Pi^A_{0|0}B_0 \left|\phi\right\rangle \\ &= -\Pi^A_{0|0}C_1\Pi^A_{0|0}C_0 \left|\phi\right\rangle \qquad (4.21)\end{aligned}$$

This suggests that C_0 and C_1 also have the anti-commutativity when acting on $\left|\phi\right\rangle$ subject to the projector $\Pi^A_{0|0}$.

With similar argument, we can also derive

$$\Pi^B_{0|0}\{A_0, A_1\} \left|\phi\right\rangle = 0, \qquad (4.22)$$

$$\Pi^B_{0|0}\{C_0, C_1\} \left|\phi\right\rangle = 0, \qquad (4.23)$$

Now we could start to define our local isometry. To define the isometry, we need the control operator. However, before we define the isometry, it is not bad to try to estimate the output of an isometry in the tripartite case. The local operation at each party is the same as that in Figure 2.1. Then for an arbitrary state $\left|\phi\right\rangle$,

$$\begin{aligned}&\Psi(\left|\phi\right\rangle_{\mathcal{ABC}} \otimes \left|000\right\rangle_{\mathcal{A'B'C'}})\\ =&\Pi^A_0\Pi^B_0\Pi^C_0 \left|\phi\right\rangle \left|000\right\rangle + \Pi^A_0\Pi^B_0 X_C\Pi^C_1 \left|\phi\right\rangle \left|001\right\rangle\\ +&\Pi^A_0 X_B\Pi^B_1\Pi^C_0 \left|\phi\right\rangle \left|010\right\rangle + \Pi^A_0 X_B\Pi^B_1 X_C\Pi^C_1 \left|\phi\right\rangle \left|011\right\rangle\\ +&X_A\Pi^A_1\Pi^B_0\Pi^C_0 \left|\phi\right\rangle \left|100\right\rangle + X_A\Pi^A_1\Pi^B_0 X_C\Pi^C_1 \left|\phi\right\rangle \left|101\right\rangle\\ +&X_A\Pi^A_1 X_B\Pi^B_1\Pi^C_0 \left|\phi\right\rangle \left|110\right\rangle + X_A\Pi^A_1 X_B\Pi^B_1 X_C\Pi^C_1 \left|\phi\right\rangle \left|111\right\rangle , \qquad (4.24)\end{aligned}$$

where $\Pi_{a/b/c}^{A/B/C}$ is the projector of $Z_{A/B/C}$. This is the general output of any given isometry.

We propose the following definition for the control operators

$$\begin{aligned} Z_A &= A_0, & X_A &= A_1, \\ Z_B &= B_0, & X_B &= B_1, \\ Z_C &= C_0, & X_C &= C_1. \end{aligned} \tag{4.25}$$

With such definition, one could check that the isometry (4.24) preserves the inner product of any input states,

$$\Psi^\dagger(|\phi'\rangle \otimes |000\rangle)\Psi(|\phi\rangle \otimes |000\rangle) = \langle \phi'|\phi\rangle\,, \tag{4.26}$$

this is also due to the fact all the control operators defined are unitary.

With the property (4.8), we know that in the sum of the above output of the isometry, only three of the terms will remain, which gives

$$\begin{aligned} &\Psi(|\phi\rangle_{\mathcal{ABC}} \otimes |000\rangle_{\mathcal{A'B'C'}}) \\ =&\Pi^A_{0|0}\Pi^B_{0|0}X_C\Pi^C_{1|0}\,|\phi\rangle\,|001\rangle + \Pi^A_{0|0}X_B\Pi^B_{1|0}\Pi^C_{0|0}\,|\phi\rangle\,|010\rangle + X_A\Pi^A_{1|0}\Pi^B_{0|0}\Pi^C_{0|0}\,|\phi\rangle\,|100\rangle\,. \end{aligned} \tag{4.27}$$

In addition, for any party, for instance A,

$$X_A\Pi^A_1\,|\phi\rangle = X_A\frac{\mathbb{1}-Z_A}{2}\,|\phi\rangle = \frac{\mathbb{1}+Z_A}{2}X_A\,|\phi\rangle = \Pi^A_0 X_A\,|\phi\rangle\,. \tag{4.28}$$

Thus, for the system satisfying the statistics in Theorem 10,

$$\begin{aligned} &\Psi(|\phi\rangle_{\mathcal{ABC}} \otimes |000\rangle_{\mathcal{A'B'C'}}) \\ =&\Pi^A_{0|0}\Pi^B_{0|0}X_C\Pi^C_{1|0}\,|\phi\rangle\,|001\rangle + \Pi^A_{0|0}X_B\Pi^B_{1|0}\Pi^C_{0|0}\,|\phi\rangle\,|010\rangle + X_A\Pi^A_{1|0}\Pi^B_{0|0}\Pi^C_{0|0}\,|\phi\rangle\,|100\rangle \\ =&\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}X_C\,|\phi\rangle\,|001\rangle + \Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}X_B\,|\phi\rangle\,|010\rangle + \Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}X_A\,|\phi\rangle\,|100\rangle \end{aligned}$$

$$
\begin{aligned}
&=\sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}X_B\left|\phi\right\rangle \frac{|001\rangle+|010\rangle+|100\rangle}{\sqrt{3}}.\\
&=\left|\text{junk}\right\rangle_{\mathcal{ABC}}\left|W_3\right\rangle_{\mathcal{A}'\mathcal{B}'\mathcal{C}'}. \qquad (4.29)
\end{aligned}
$$

which successfully extracts a $|W_3\rangle$ state out of the system that is compatible with the criterion. □

4.1.2 Robustness

Now we are going to discuss the robustness of the self-testing of the $|W_3\rangle$ state. As we have defined before, the study of the robustness is to estimate how close the system is to the ideal $|W_3\rangle$ state if the experimental data is not perfectly matching the criterion showing in Theorem 10. That is to say, if

$$|\left\langle\phi\right|\Pi^A_{a|x}\Pi^B_{b|y}\Pi^C_{c|z}\left|\phi\right\rangle-\tilde{p}(abc|xyz)|\leq\varepsilon, \qquad (4.30)$$

where $\tilde{p}(abc|xyz)$ is the statistics given in Theorem 10 for the ideal case, how close is the output state of the isometry compared to the output in the ideal case? In another way to say, we hope to see what is the fidelity of the ancillary qubits with that of the ideal case,

$$F=F(\varepsilon)=\|\langle\tilde{\varphi}|\varphi\rangle\|^2, \qquad (4.31)$$

where $|\tilde{\varphi}\rangle$ and $|\varphi\rangle$ correspond to the output state of the ancillary qubits in the ideal case and nonideal case.

We could in principle follow the procedure as that of section 2.2 to have an analytical expression of $F(\varepsilon)$. However, we will simply give the analytical bound here without discussion in detail,

$$F\geq 1-12.35\varepsilon^{\frac{1}{2}}-2944.2\varepsilon-185.25\varepsilon^{\frac{5}{4}}. \qquad (4.32)$$

For detailed proof, please refer to Appendix A and [55].

On the contrary, we will use the SDP method to get a robustness bound directly, both because of it simplicity and better performance.

For the isometry, it is obvious that a proper one will be (4.24) with control operators (4.25). Thus, the formalism of SDP will be

$$\begin{aligned} \min \quad & F(S) \\ \text{such that} \quad & |\langle\phi|\,\Pi^A_{a|x}\Pi^B_{b|y}\Pi^C_{c|z}\,|\phi\rangle - \tilde{p}(abc|xyz)| \leq \varepsilon, \\ & \Gamma(S) \geq 0. \end{aligned} \tag{4.33}$$

We choose the sequence S to be the S_2 removed some of the terms, which is

$$\begin{aligned} S = \{&\mathbb{1}, A_x, B_y, C_z, A_xB_yC_z, A_xB_y, A_xC_z, B_yC_z, A_xA_{x'}, B_yB_{y'}, C_zC_{z'}, \\ &A_xA_{x'}B_yB_{y'}, B_yB_{y'}C_zC_{z'}, A_xA_{x'}C_zC_{z'}, A_xA_{x'}B_yB_{y'}C_zC_{z'}\}. \end{aligned} \tag{4.34}$$

With all these components ready, we get the robustness bound as the following,

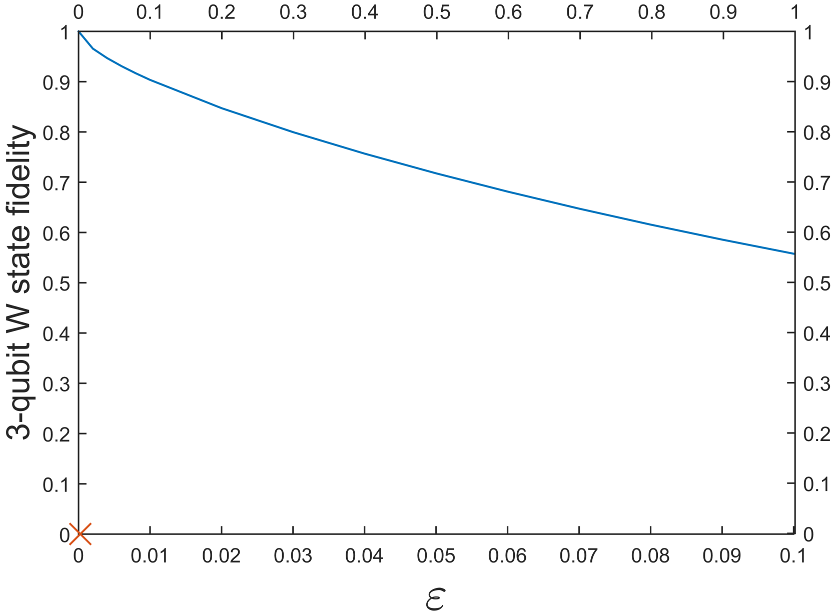


Figure 4.2: Robustness bound as a function of ε for 3-qubit W state. As a comparison, we put a red cross on the x axis, where $\varepsilon = 0.000265$, that gives zero fidelity with result from analytical method.

For comparison, we put a red cross on the x axis, where $\varepsilon = 0.000265$, that gives zero fidelity with result from analytical method (4.32). As the plot showing, the bound from the SDP is much better than the one from the analytical method.

4.2 Self-testing of N-qubit W state

Since we have shown in the previous section that the self-testing of 3-qubit W state can be achieved, we now ask the question that whether this result could be generalized to N-qubit W state. The answer turns out to be yes, and we will state the result below.

Theorem 11. *Suppose there are N parties, A^1, A^2,..., A^{n-1} and A^n. A^1, A^2,..., A^{n-1} each can perform two measurements labelled by $x_1, x_2, ..., x_{n-1} \in \{0.1\}$, A^n can perform three measurements labelled by $x_n \in \{0,1,2\}$. After measuring on an unknown shared quantum state $|\phi\rangle$, each of them produces binary outcomes labelled by $a_1, a_2, ..., a_n \in \{0,1\}$. The $|W_n\rangle$ state is self-tested if the following statistics are observed:*

$$\langle\phi|\, \Pi^k_{1|0} \prod_{i\neq k} \Pi^i_{0|0} \,|\phi\rangle = \frac{1}{n}, \qquad k = 1,2,...,n, \tag{4.35}$$

$$\begin{cases} \langle\phi|\, A^j_0 A^n_0 \prod_{i\neq j,n} \Pi^i_{0|0} \,|\phi\rangle = -\langle\phi|\, A^j_1 A^n_1 \prod_{i\neq j,n} \Pi^i_{0|0} \,|\phi\rangle = -\dfrac{2}{n}, \\ \langle\phi|\, A^j_1 A^n_0 \prod_{i\neq j,n} \Pi^i_{0|0} \,|\phi\rangle = \langle\phi|\, A^j_0 A^n_1 \prod_{i\neq j,n} \Pi^i_{0|0} \,|\phi\rangle = 0, \\ \langle\phi|\, A^j_0 A^n_2 \prod_{i\neq j,n} \Pi^i_{0|0} \,|\phi\rangle = -\langle\phi|\, A^j_1 A^n_2 \prod_{i\neq j,n} \Pi^i_{0|0} \,|\phi\rangle = -\dfrac{\sqrt{2}}{n}, \end{cases} \tag{4.36}$$

$$j = 1,2,...,n-1, \tag{4.37}$$

where the superscripts represent the indexes of the parties and A_{x_i} is the measurement operator associated to each party.

Proof. Due to the similarity to the 3-qubit W state self-testing, the proof of the N-

qubit W state self-testing is actually quite similar to the proof of the 3-qubit case. Since the key point of proving a self-testing is to define proper control operators at each party that anti-commute to each other, we will derive such a pair of operators for each party and skip the rest of the proof. One could simply complete the proof with the isometry for N parties once having the anti-commutative operators.

From the statistics (4.35), we know that $\langle\phi| \prod_{i=1}^{n} \Pi^i_{a_i|x_i} |\phi\rangle = 0$ if $\sum_i a_i \neq 1$. It is also a good idea to carry out the following estimation

$$\|A^j_{x_j} \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle \| = \sqrt{\| \langle\phi| \prod_{i\neq j,n} \Pi^i_{0|0} (A^j_{x_j})^\dagger A^j_{x_j} \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle \|}$$

$$= \sqrt{\| \langle\phi| \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle \|} = \sqrt{\frac{2}{n}}. \tag{4.38}$$

With the observation (4.36), we will carry out similar estimation as (4.12).

$$-\frac{2}{n} = \langle\phi| \prod_{i\neq j,n} \Pi^i_{0|0} A^j_0 A^n_0 \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle$$

$$= \|A^j_0 \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle \| \cdot \|A^n_0 \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle \| \cdot \cos(\theta)$$

$$= \sqrt{\frac{2}{n}} \cdot \sqrt{\frac{2}{n}} \cos(\theta), \tag{4.39}$$

where $\theta = \angle(A^j_0 \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle, A^n_0 \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle)$ and $\angle(,)$ represents the angle between the two vectors in the parentheses. This shows that

$$\angle(A^j_0 \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle, A^n_0 \prod_{i\neq j,n} \Pi^i_{0|0} |\phi\rangle) = \pi. \tag{4.40}$$

With similar calculation, we get

$$\angle(A_1^j \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle, A_1^n \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle) = 0, \tag{4.41}$$

$$\angle(A_1^j \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle, A_0^n \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle) = \frac{\pi}{2}, \tag{4.42}$$

$$\angle(A_0^j \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle, A_1^n \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle) = \frac{\pi}{2}, \tag{4.43}$$

$$\angle(A_0^j \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle, A_2^n \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle) = \frac{3\pi}{4}, \tag{4.44}$$

$$\angle(A_1^j \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle, A_2^n \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle) = \frac{\pi}{4}. \tag{4.45}$$

With such relation of these vectors, the only case that could happen is as the following, as all the vectors are in the same plane.

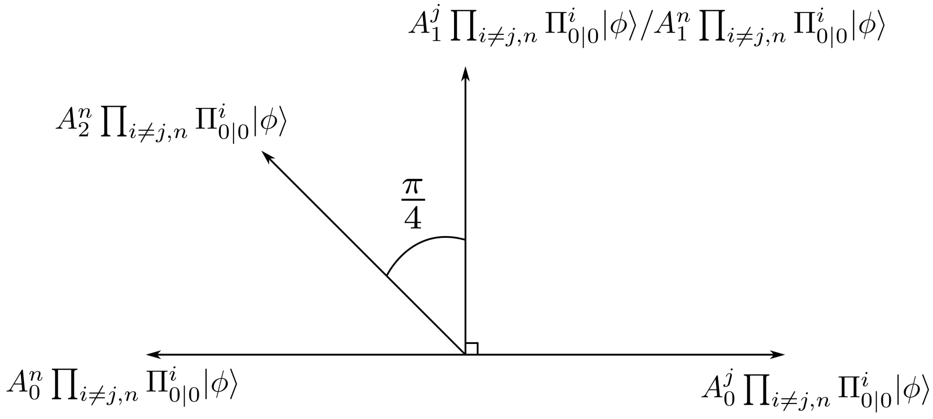

$A_1^j \prod_{i\neq j,n} \Pi_{0|0}^i|\phi\rangle / A_1^n \prod_{i\neq j,n} \Pi_{0|0}^i|\phi\rangle$
$A_2^n \prod_{i\neq j,n} \Pi_{0|0}^i|\phi\rangle$
$\frac{\pi}{4}$
$A_0^n \prod_{i\neq j,n} \Pi_{0|0}^i|\phi\rangle$
$A_0^j \prod_{i\neq j,n} \Pi_{0|0}^i|\phi\rangle$

Figure 4.3: Configuration of vectors in the space for N-qubit W state.

This means

$$\begin{aligned} A_2^n \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle &= \frac{A_1^j \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle - A_0^j \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle}{\sqrt{2}} \\ &= \frac{A_0^n \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle + A_1^n \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle}{\sqrt{2}}. \end{aligned} \tag{4.46}$$

Applying $A_2^n \prod_{i\neq j,n} \Pi_{0|0}^i$ on both side of the equation, we get

$$A_2^n A_2^n \prod_{i\neq j,n} \Pi_{0|0}^i \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle = A_2^n \prod_{i\neq j,n} \Pi_{0|0}^i \frac{A_1^j \prod_{i\neq j,n} \Pi_{0|0}^i - A_0^j \prod_{i\neq j,n} \Pi_{0|0}^i}{\sqrt{2}} \left|\phi\right\rangle$$

$$= \frac{A_1^j \prod_{i\neq j,n} \Pi_{0|0}^i - A_0^j \prod_{i\neq j,n} \Pi_{0|0}^i}{\sqrt{2}} A_2^n \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle$$

$$= \left(\frac{A_1^j \prod_{i\neq j,n} \Pi_{0|0}^i - A_0^j \prod_{i\neq j,n} \Pi_{0|0}^i}{\sqrt{2}} \right)^2 \left|\phi\right\rangle$$

$$= \left(\frac{(A_1^j)^2 \prod_{i\neq j,n} \Pi_{0|0}^i + (A_0^j)^2 \prod_{i\neq j,n} \Pi_{0|0}^i}{2} - \frac{1}{2}\{A_0^j, A_1^j\} \prod_{i\neq j,n} \Pi_{0|0}^i \right) \left|\phi\right\rangle ,$$

$$= \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle - \frac{1}{2}\{A_0^j, A_1^j\} \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle , \tag{4.47}$$

which simply means

$$\{A_0^j, A_1^j\} \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle = 0. \tag{4.48}$$

This shows the anti-commutativity of A_0^j and A_1^j subjective to the projection $\prod_{i\neq j,n} \Pi_{0|0}^i$. With similar argument, we could also prove

$$\{A_0^n, A_1^n\} \prod_{i\neq j,n} \Pi_{0|0}^i \left|\phi\right\rangle = 0. \tag{4.49}$$

These are all the essentials we need to complete the rest of the proof. □

4.3 Self-testing of 3-qubit states in general

In the previous two sections, we show that W state can be self-tested. It is easy to generalize the 3-qubit W state self-testing to N-qubit since there exists some certain simplicity in the form of the state itself. In this section, we seek the possibility of self-testing states that may not be as simple as a W state.

We try to get inspirations from the way we did in the W state self-testing. By scrutinizing the criteria in the W state self-testing, we notice that, the idea behind them is to first project the state into a state that has entanglement in two parties, then, one could apply the bipartite self-testing to these two parties. Hence, the key point is that the state should have a structure which would allow us to follow the similar procedure as we had in the W state self-testing.

Fortunately, a result of the study on generalized Schmidt decomposition of 3-qubit state [88] sheds light on our problem. For a 3-qubit state, up to local unitaries, it can be generally written as

$$|\phi\rangle_{\mathcal{ABC}} = \lambda_0 |000\rangle + \lambda_1 e^{i\theta} |100\rangle + \lambda_2 |101\rangle + \lambda_3 |110\rangle + \lambda_4 |111\rangle . \tag{4.50}$$

Depending on the values of λ_is and θ, the state will be in different classes. Among those, there are the class of product states, biseparable states and generalized (extended) GHZ states. It is easy to see that the method which arises from the W state self-testing will not work on these state. We will then skip the study of these classes and only concentrate on the rest of the states. Since it is still not clear whether the phase could be self-tested or not in the 3-qubit case, to simplify, we will only consider the case where $\theta = 0$. Specifically, we will study the cases which

$$\begin{cases} \lambda_0 \neq 0, \qquad \text{the number of } (\lambda_i = 0) = 1, \qquad i = 1,2,3,4, & (4.51) \\ \lambda_0\lambda_2\lambda_3 \neq 0, \qquad \lambda_1 = \lambda_4 = 0. & (4.52) \end{cases}$$

We can rewrite the state as

$$|\phi\rangle = \lambda_0 |000\rangle_{\mathcal{ABC}} + |1\rangle_{\mathcal{A}} (\lambda_1 |00\rangle + \lambda_2 |01\rangle + \lambda_3 |10\rangle + \lambda_4 |11\rangle)_{\mathcal{BC}}. \tag{4.53}$$

For the λ_is satisfying (4.51) or (4.52), there exists a Schmidt decomposition for the state inside the parentheses,

$$|\phi\rangle = \lambda_0 |000\rangle + \sqrt{1-\lambda_0^2}\, |1\rangle_{\mathcal{A}} \left(\cos\alpha_{\mathcal{A}} |0'_{\mathcal{B}} 0'_{\mathcal{C}}\rangle + \sin\alpha_{\mathcal{A}} |1'_{\mathcal{B}} 1'_{\mathcal{C}}\rangle \right), \tag{4.54}$$

where as $\lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2 = 1$ and $|0'_{\mathcal{B}/\mathcal{C}}\rangle$, $|1'_{\mathcal{B}/\mathcal{C}}\rangle$ are the bases of A and B after the Schmidt decomposition.

On the other hand, if we rewrite the state to single out the party B or C

$$|\phi\rangle = |0\rangle_{\mathcal{B}} \left(\lambda_0 |00\rangle + \lambda_1 |10\rangle + \lambda_2 |11\rangle \right)_{\mathcal{AC}} + |1\rangle_{\mathcal{B}} \left(\lambda_3 |10\rangle + \lambda_4 |11\rangle \right)_{\mathcal{AC}}, \tag{4.55}$$

$$|\phi\rangle = |0\rangle_{\mathcal{C}} \left(\lambda_0 |00\rangle + \lambda_1 |10\rangle + \lambda_3 |11\rangle \right)_{\mathcal{AB}} + |1\rangle_{\mathcal{C}} \left(\lambda_2 |10\rangle + \lambda_4 |11\rangle \right)_{\mathcal{AB}}. \tag{4.56}$$

Depending on whether $\lambda_1 = 0$, $\lambda_2 = 0$ or $\lambda_3 = 0$, one can choose to single out B or C. Let us say $\lambda_3 = 0$, then we will choose the partition (4.55). Obviously, the state in the first parentheses will have a Schmidt decomposition,

$$|\phi\rangle = |0\rangle_{\mathcal{B}} \left(\lambda_0 |00\rangle + \lambda_1 |10\rangle + \lambda_2 |11\rangle \right)_{\mathcal{AC}} + \lambda_4 |1\rangle_{\mathcal{B}} |11\rangle_{\mathcal{AC}}$$

$$= \sqrt{1-\lambda_4^2}\, |0\rangle_{\mathcal{B}} \left(\cos\alpha_{\mathcal{B}} |0'_{\mathcal{A}} 0''_{\mathcal{C}}\rangle + \sin\alpha_{\mathcal{B}} |1'_{\mathcal{A}} 1''_{\mathcal{C}}\rangle \right)_{\mathcal{AC}} + \lambda_4 |1\rangle_{\mathcal{B}} |11\rangle_{\mathcal{AC}}\,, \tag{4.57}$$

where $|0'_{\mathcal{A}}\rangle$, $|1'_{\mathcal{A}}\rangle$, $|0''_{\mathcal{C}}\rangle$ and $|1''_{\mathcal{C}}\rangle$ are the bases of A and C after the Schmidt decomposition.

With the partition (4.54) and (4.57), we could come up with the criterion for the self-testing of the state. First, we can project the state of A into $|1\rangle$ and perform a self-testing of the partially entangled state $|\alpha_{\mathcal{A}}\rangle$ in a rotated basis. Then, we project the state of B or C into $|0\rangle$ depending on whether $\lambda_1 = 0$, $\lambda_2 = 0$ or $\lambda_3 = 0$, and perform a self-testing of the partially entangled state $|\alpha_{\mathcal{B}/\mathcal{C}}\rangle$ in a rotated basis. We are supposed to get the self-testing of the state after these two steps, however, it still need to be verified.

One thing which should be discussed here is that, for a self-testing of a partially entangled state, the measurement setting is not arbitrary. Hence, the measurements we choose on A, B and C should satisfy the constraints set by the self-testing of partially entangled state simultaneously with different partitions. It is quite subtle to state the exact relation of the measurement settings and the parameters λ_is, therefore, we will give an example state and show the process to find the proper measurement settings.

Let us take the following state as an example

$$|\phi\rangle_{\mathcal{ABC}} = \frac{1}{2\sqrt{77}}\big(9\,|000\rangle + 5\,|100\rangle + 9\,|101\rangle + 11\,|111\rangle\,\big)_{\mathcal{ABC}}. \tag{4.58}$$

where we set $\lambda_3 = 0$. With such a state, the partitions (4.53) and (4.55) will become

$$|\phi\rangle = \frac{9}{2\sqrt{77}}\,|000\rangle_{\mathcal{ABC}} + \frac{1}{2}\sqrt{\frac{227}{77}}\,|1\rangle_{\mathcal{A}}\,\big(\frac{5}{\sqrt{227}}\,|00\rangle + \frac{9}{\sqrt{227}}\,|01\rangle + \frac{11}{\sqrt{227}}\,|11\rangle\,\big)_{\mathcal{BC}}, \tag{4.59}$$

$$|\phi\rangle = \frac{1}{2}\sqrt{\frac{17}{7}}\,|0\rangle_{\mathcal{B}}\,\big(\frac{9}{\sqrt{187}}\,|00\rangle + \frac{5}{\sqrt{187}}\,|10\rangle + \frac{9}{\sqrt{187}}\,|11\rangle\,\big)_{\mathcal{AC}} + \frac{11}{2\sqrt{77}}\,|1\rangle_{\mathcal{B}}\,|11\rangle_{\mathcal{AC}}\,. \tag{4.60}$$

Now we can perform the Schmidt decompositions inside the parentheses of these two partitions. For the partition which singles out A,

$$|\phi\rangle = \frac{9}{2\sqrt{77}}\,|000\rangle_{\mathcal{ABC}} + \frac{1}{2}\sqrt{\frac{227}{77}}\,|1\rangle_{\mathcal{A}}\,\big(\cos\alpha_{\mathcal{A}}\,|0'_{\mathcal{B}}0'_{\mathcal{C}}\rangle + \sin\alpha_{\mathcal{A}}\,|1'_{\mathcal{B}}1'_{\mathcal{C}}\rangle\,\big)_{\mathcal{BC}}, \tag{4.61}$$

where $\alpha_{\mathcal{A}} = 14.492528461873206°$, and

$$|i'_{\mathcal{B}}\rangle = U_{\mathcal{B}}\,|i\rangle_{\mathcal{B}}\,, \tag{4.62}$$

$$|i'_{\mathcal{C}}\rangle = V_{\mathcal{C}}\,|i\rangle_{\mathcal{C}}\,, \tag{4.63}$$

$$U_{\mathcal{B}} = \begin{pmatrix} -0.679874579341885 & -0.733328409626066 \\ -0.733328409626066 & 0.679874579341885 \end{pmatrix}, \tag{4.64}$$

$$V_{\mathcal{C}} = \begin{pmatrix} -0.233039556506182 & -0.972467256571347 \\ -0.972467256571347 & 0.233039556506182 \end{pmatrix}. \tag{4.65}$$

For the partition which singles out B,

$$|\phi\rangle = \frac{1}{2}\sqrt{\frac{17}{7}}\,|0\rangle_{\mathcal{B}}\left(\cos\alpha_{\mathcal{B}}\,|0'_{\mathcal{A}}0''_{\mathcal{C}}\rangle + \sin\alpha_{\mathcal{B}}\,|1'_{\mathcal{A}}1''_{\mathcal{C}}\rangle\right)_{\mathcal{AC}} + \frac{11}{2\sqrt{77}}\,|1\rangle_{\mathcal{B}}\,|11\rangle_{\mathcal{AC}}\,, \tag{4.66}$$

where $\alpha_{\mathcal{B}} = 30.016323409628981°$, and

$$|i'_{\mathcal{A}}\rangle = U'_{\mathcal{A}}\,|i\rangle_{\mathcal{A}}\,, \tag{4.67}$$

$$|i''_{\mathcal{C}}\rangle = V'_{\mathcal{C}}\,|i\rangle_{\mathcal{C}}\,, \tag{4.68}$$

$$U'_{\mathcal{A}} = \begin{pmatrix} 0.605126489344957 & 0.796129343695512 \\ -0.796129343695512 & 0.605126489344957 \end{pmatrix}, \tag{4.69}$$

$$V'_{\mathcal{C}} = \begin{pmatrix} 0.796129343695512 & 0.605126489344957 \\ -0.605126489344957 & 0.796129343695512 \end{pmatrix}. \tag{4.70}$$

Hence, the proper measurement settings will be able to self-test this two partially entangled state after this two sets of transformations. A possible measurement settings will be the following

$$\begin{aligned} A_0 &= \sigma_z, & A_1 &= \sigma_x, \\ B_0 &= \sigma_z, & B_1 &= \sigma_x, \\ C_0 &= \sigma_z, & C_1 &= \sigma_x, \\ C_2 &= \frac{-\sigma_z + \sigma_x}{\sqrt{2}}. \end{aligned} \tag{4.71}$$

With these measurements and the state (4.58), we could have the ideal strategy that leads to the criterion of our self-testing.

To exam the feasibility of the criterion, we will use the SDP to verify if it really can self-test the state (4.58). Inspired from the ideal strategy above, we will define our control operators as the following

$$\begin{aligned} Z_A &= A_0, & X_A &= A_1, \\ Z_B &= B_0, & X_B &= B_1, \\ Z_C &= C_0, & X_C &= C_1. \end{aligned}$$

With all these components ready, we could write down the formalism of the SDP

$$\begin{aligned} \text{min} \quad & F(S) \\ \text{such that} \quad & \langle\phi| \Pi^A_{a|x}\Pi^B_{b|y}\Pi^C_{c|z} |\phi\rangle = \tilde{p}(abc|xyz), \\ & \Gamma(S) \geq 0, \end{aligned} \tag{4.72}$$

where $\tilde{p}$ is the probability distribution from the ideal strategy. We put the sign of the probability to be equal since we only want to know whether it self-tests the state (4.58) or not rather than the robustness.

For the state (4.58) considered here, with a SDP matrix of dimension 57, we manage to get

$$F_{\text{min}} = 0.999999610643920. \tag{4.73}$$

Thus, it is fair enough to trust the correctness of the criterion proposed above.

The reason that we still have three measurements for C is, it may happen that the measurements of C could self-test the partially entangled 2-qubit state with the measurements of B under partition (4.61), but cannot self-test with the measurements of A under partition (4.66), since they undergo different rotations according to the Schmidt decomposition. Hence, even though the third measurement on C may be redundant in some cases, we still keep it to guarantee the success of the self-testing. It turns out that the self-testing of the partially entangled state under partition (4.61) can only be achieved with at least C_2 included. In general, as long as the 3-qubit state could be written in two different partitions with valid Schmidt decompositions like (4.54) and (4.57), one could add more measurement settings on any of the parties to ensure the success of the self-testing of the bipartite partially entangled state. This will allow us to self-test all the states in the categories (4.51) and (4.52). However, it is still not clear whether the 3-qubit state with non-trivial phase involved is self-testable or not in general. We are also looking forward to future studies to cover this topic.

To summarize, we have studied a more general case of 3-qubit state self-testing. Besides the trivial states, for instance the product states and biseparable states, and the states that belong to the graph state class, with the procedure described above, we are able to self-test the states that have genuine tripartite entanglement (with real coefficients). Although it could still be possible to study the behaviour of the quantum set in the tripartite case, we will skip that since the amount of computation required is much more than that of the bipartite case. Besides the methods we presented to self-test multipartite states, we are also looking forward to self-testing by inequalities, since there are actually inequalities associated to multipartite states studied before [89, 90, 91, 92, 93].

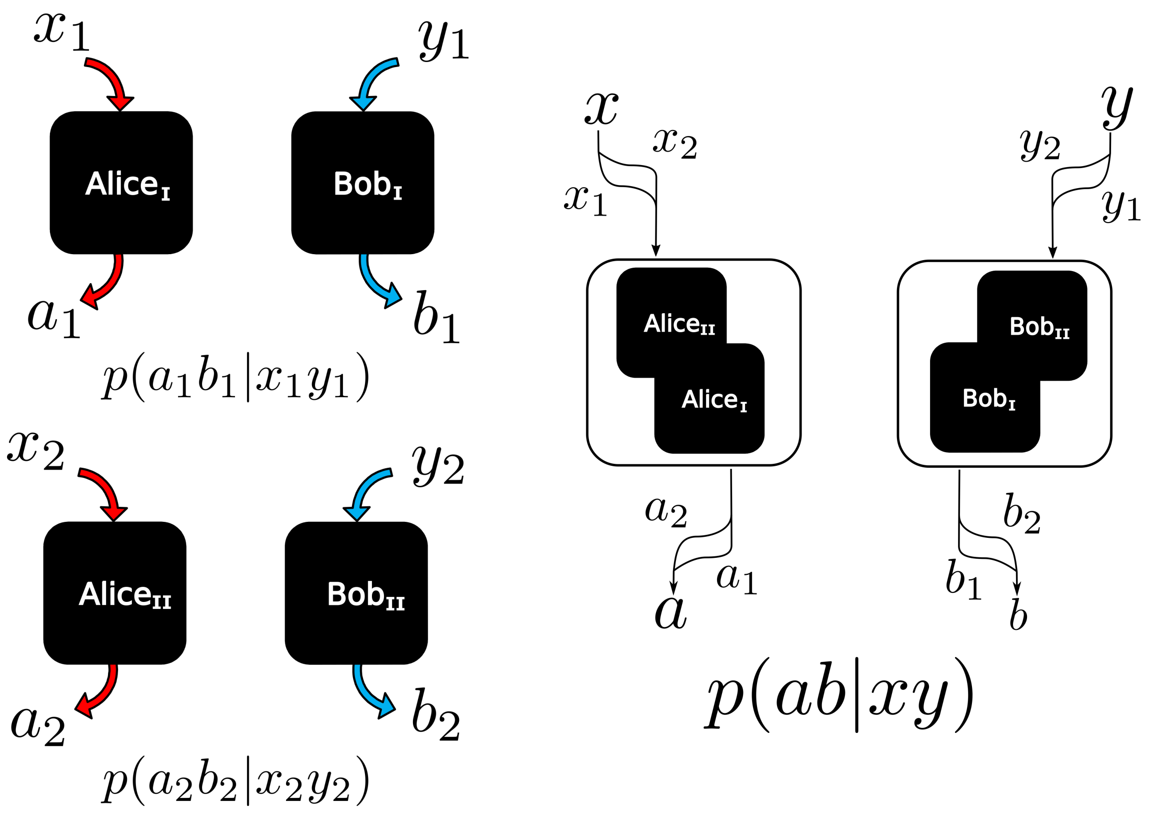
Chapter 5

Parallel self-testing of entanglement resource

In the previous chapters, our main focus is on one copy of some specific state. However, the certification of multiple copies of state becomes more and more popular recently. As in the work of [45, 94], the proposed model for quantum computing requires multiple pairs of certified singlet states. This intrigues us to study the self-testing of multiple copies of quantum states.

In general, there could be two ways to certify multiple copies of state. In terms of non-local game, it could be played either sequentially or parallelly. In the bipartite case, a sequential test means that the two parties receive the measurement settings for each copy of state sequentially and reveal the results immediately after the measurements are done. However, in the parallel case, the measurement settings for all the copies on each party arrive at the same time, and both of the parties will reveal the results of the measurements of all the copies at the same time. With these definition, it could be seen that a parallel test in fact has less restrictions on how the game is played. The two players at each party could even use the history of the results of the measurements on previous copies to mimic the behaviour of them. On the contrary, a sequential test will be much more restricted, since in each run, the players need to reveal the result of each copy and there is not to much freedom to play around compared to a parallel one. In this sense, a sequential test could also be considered as independent test of each copy. For the difference of these two games, one could refer to [95] for more details.

We are more interested in the parallel test of the state because it has less requirements of how the test is run. In fact, parallel repetitions have also been widely studied before [96, 97, 98, 99]. In this chapter, we will talk about how we could self-test multiple copies of singlet states in parallel and derive a robustness bounds that is reasonable for current experiments.



(b) Scheme of parallel CHSH test.

(a) Scheme of sequential CHSH test.

Figure 5.1: A sketch shows the difference between the sequential test of CHSH and parallel test of CHSH.

5.1 Parallel self-testing of two singlet states using CHSH

It is know that the violation of the CHSH inequality will self-test the singlet state $|\Phi^+\rangle$. The idea that comes straight forward after this fact is, can we self-test multiple pairs of singlet states in a similar manner. To put it another way, if the statistics arising from a parallel test lead to maximal violation of the CHSH inequality for each of the copies, can we say that the system is self-tested into multiple pairs of singlet states? This is different to independent test of each copy of the state since, as we have said before, in a parallel scenario the results of the measurements on some copies of the states may affect the behavior of the others.

5.1.1 Self-testing in the ideal case

For simplicity, we will study the case for two copies here first. To make it clean, the question that we are trying to answer is, given the statistics of a bipartite non-local game

$$p(a_1a_2b_1b_2|x_1x_2y_1y_2), \tag{5.1}$$

where $a_1, a_2, x_1, x_2 \in \{0, 1\}$ are the outputs and inputs of the first and second subsystems of A and similar for B, if p leads to the maximal violation of the CHSH inequality on each of the subsystems 1 and 2,

$$\mathcal{B}_{\text{CHSH}}(p(a_1b_1|x_1y_1)) = 2\sqrt{2}, \tag{5.2}$$

$$\mathcal{B}_{\text{CHSH}}(p(a_2b_2|x_2y_2)) = 2\sqrt{2}, \tag{5.3}$$

can we claim that the subsystems 1 and 2 are self-tested into two singlet states simultaneously?

Unfortunately, the answer to this question is no. The reason for this is simple, one may notice that, to violate the CHSH inequality, for instance (5.2), the probability

$p(a_1b_1|x_1y_1)$ actually takes four different values depending on which one it is chosen from $p(a_1b_1|x_1x_2y_1y_2)$. If one of the $p(a_1b_1|x_1x_2y_1y_2)$ is chosen, then the other three will be free to change but still violates the CHSH inequalities maximally, which will not be compatible with the statistics of that from the two singlets case. Thus, to promise the system really behaves the same way as two singlets measured by corresponding measurements, we need to require all the probabilities to be the same as that from the two singlet ones. With this adjustment, we have the main results as below

Theorem 12. *A and B both choose one four-outcome measurements out of four and we denote their choices as $x \in \{0,1,2,3\}$ and $y \in \{0,1,2,3\}$, where x and y are the decimal representations of $\overline{x_1x_2}$ and $\overline{y_1y_2}$. The outputs of A and B will be denoted by $a \in \{0,1,2,3\}$ and $b \in \{0,1,2,3\}$, where a and b are the decimal representations of $\overline{a_1a_2}$ and $\overline{b_1b_2}$. The observed statistics $p(ab|xy)$ will self-test two copies of singlet states if it is given by*

$$p(ab|xy) = \mathrm{Tr}[|\Phi^+\Phi^+\rangle\langle\Phi^+\Phi^+|\, A_x^* B_y], \tag{5.4}$$

where

$$\begin{aligned}
A_0^* &= \sigma_z \otimes \sigma_z, & A_1^* &= \sigma_z \otimes \sigma_x, \\
A_3^* &= \sigma_x \otimes \sigma_z, & A_4^* &= \sigma_x \otimes \sigma_x, \\
B_0^* &= \frac{\sigma_z - \sigma_x}{\sqrt{2}} \otimes \frac{\sigma_z - \sigma_x}{\sqrt{2}}, & B_1^* &= \frac{\sigma_z - \sigma_x}{\sqrt{2}} \otimes \frac{\sigma_z + \sigma_x}{\sqrt{2}}, \\
B_2^* &= \frac{\sigma_z + \sigma_x}{\sqrt{2}} \otimes \frac{\sigma_z - \sigma_x}{\sqrt{2}}, & B_3^* &= \frac{\sigma_z + \sigma_x}{\sqrt{2}} \otimes \frac{\sigma_z + \sigma_x}{\sqrt{2}}.
\end{aligned} \tag{5.5}$$

Before continuing, there is actually a simplification that could make the problem look cleaner. For the ideal strategy (5.4) with (5.5), we could apply a rotation $R_y(\frac{\pi}{4})$ to each of the subsystems on party B, the state and measurement settings will now become

$$|\tilde{\varphi}\rangle = \left(\cos(\frac{\pi}{8})\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \sin(\frac{\pi}{8})\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right), \tag{5.6}$$

and

$$\begin{aligned} A_0 &= \sigma_z \otimes \sigma_z, & A_1 &= \sigma_z \otimes \sigma_x, \\ A_3 &= \sigma_x \otimes \sigma_z, & A_4 &= \sigma_x \otimes \sigma_x, \\ B_0 &= \sigma_z \otimes \sigma_z, & B_1 &= \sigma_z \otimes \sigma_x, \\ B_3 &= \sigma_x \otimes \sigma_z, & B_4 &= \sigma_x \otimes \sigma_x. \end{aligned} \tag{5.7}$$

In the following proof, we will simply use the above settings.

Proof. To prove the self-testing of the state (5.6), basically we need to derive four pairs of anti-commutative operators on each of the supposed qubit subsystems. With these operators, we can then define a valid isometry that can turn the state of the system into the ideal state (5.6). Now suppose $\Pi_{a|x}$ and $\Pi_{b|y}$ are the projectors for the measurement operators on A and B. Inspired from the ideal strategy, we could define the operators below which are supposed to be the σ_z and σ_x operations on the four subsystems:

$$Z_{\mathcal{A}_1} := \Pi^A_{0|0} + \Pi^A_{1|0} - \Pi^A_{2|0} - \Pi^A_{3|0} \tag{5.8}$$

$$Z_{\mathcal{A}_2} := \Pi^A_{0|0} - \Pi^A_{1|0} + \Pi^A_{2|0} - \Pi^A_{3|0} \tag{5.9}$$

$$X_{\mathcal{A}_1} := \Pi^A_{0|3} + \Pi^A_{1|3} - \Pi^A_{2|3} - \Pi^A_{3|3} \tag{5.10}$$

$$X_{\mathcal{A}_2} := \Pi^A_{0|3} - \Pi^A_{1|3} + \Pi^A_{2|3} - \Pi^A_{3|3} \tag{5.11}$$

$$
\begin{aligned}
Z'_{\mathcal{A}_1} &:= \Pi^A_{0|2} + \Pi^A_{1|2} - \Pi^A_{2|2} - \Pi^A_{3|2} && (5.12)\\
Z'_{\mathcal{A}_2} &:= \Pi^A_{0|1} - \Pi^A_{1|1} + \Pi^A_{2|1} - \Pi^A_{3|1} && (5.13)\\
X'_{\mathcal{A}_1} &:= \Pi^A_{0|1} + \Pi^A_{1|1} - \Pi^A_{2|1} - \Pi^A_{3|1} && (5.14)\\
X'_{\mathcal{A}_2} &:= \Pi^A_{0|2} - \Pi^A_{1|2} + \Pi^A_{2|2} - \Pi^A_{3|2} && (5.15)
\end{aligned}
$$

$$
\begin{aligned}
2Z_{\mathcal{B}_1} &:= \Pi^B_{0|0} + \Pi^B_{1|0} - \Pi^B_{2|0} - \Pi^B_{3|0} \\
&\quad +\Pi^B_{0|2} + \Pi^B_{1|2} - \Pi^B_{2|2} - \Pi^B_{3|2} && (5.16)\\
2Z_{\mathcal{B}_2} &:= \Pi^B_{0|0} - \Pi^B_{1|0} + \Pi^B_{2|0} - \Pi^B_{3|0} \\
&\quad +\Pi^B_{0|1} - \Pi^B_{1|1} + \Pi^B_{2|1} - \Pi^B_{3|1} && (5.17)
\end{aligned}
$$

$$
\begin{aligned}
2X_{\mathcal{B}_1} &:= \Pi^B_{0|3} + \Pi^B_{1|3} - \Pi^B_{2|3} - \Pi^B_{3|3} \\
&\quad +\Pi^B_{0|1} + \Pi^B_{1|1} - \Pi^B_{2|1} - \Pi^B_{3|1} && (5.18)\\
2X_{\mathcal{B}_2} &:= \Pi^B_{0|3} - \Pi^B_{1|3} + \Pi^B_{2|3} - \Pi^B_{3|3} \\
&\quad \Pi^B_{0|2} - \Pi^B_{1|2} + \Pi^B_{2|2} - \Pi^B_{3|2} && (5.19)
\end{aligned}
$$

The subscripts $\mathcal{A}_{1/2}$ and $\mathcal{B}_{1/2}$ denote the first and second sub-qubits that are supposed to be in the state for A and B. From the ideal strategy (5.7), we see that actually one can have different expressions for the σ_z and σ_x on any of the qubit subsystems. This is why we have Z and Z' in the above definition. For B, Z and X could be considered as the average effects of two different possible definitions of σ_z and σ_x.

By construction,

$$
\begin{aligned}
&[Z_{\mathcal{A}_1}, Z_{\mathcal{A}_2}] = 0, && [X_{\mathcal{A}_1}, X_{\mathcal{A}_2}] = 0,\\
&[Z'_{\mathcal{A}_1}, X'_{\mathcal{A}_2}] = 0, && [X'_{\mathcal{A}_1}, Z'_{\mathcal{A}_2}] = 0.
\end{aligned}
\qquad (5.20)
$$

Also, from the definitions of V, and W, we could see that the eigenvalues are bounded between -1 and 1 since their norms are all equal or less than 1.

Imagining the correlations of the real experiment achieve the maximal violation of CHSH on each pair of the subsystems that are supposed to be singlets, which are,

$$\frac{1}{2}\langle\phi|\left[\left(Z_{\mathcal{A}_1}+Z'_{\mathcal{A}_1}\right)\left(Z_{\mathcal{B}_1}+X_{\mathcal{B}_1}\right)+\left(X_{\mathcal{A}_1}+X'_{\mathcal{A}_1}\right)\left(Z_{\mathcal{B}_1}-X_{\mathcal{B}_1}\right)\right]|\phi\rangle = 2\sqrt{2} \tag{5.21}$$

$$\frac{1}{2}\langle\phi|\left[\left(Z_{\mathcal{A}_2}+Z'_{\mathcal{A}_2}\right)\left(Z_{\mathcal{B}_2}+X_{\mathcal{B}_2}\right)+\left(X_{\mathcal{A}_2}+X'_{\mathcal{A}_2}\right)\left(Z_{\mathcal{B}_2}-X_{\mathcal{B}_2}\right)\right]|\phi\rangle = 2\sqrt{2}. \tag{5.22}$$

These can be decomposed into four separate inequalities:

$$\langle\phi|\left[Z_{\mathcal{A}_1}\left(Z_{\mathcal{B}_1}+X_{\mathcal{B}_1}\right)+X_{\mathcal{A}_1}\left(Z_{\mathcal{B}_1}-X_{\mathcal{B}_1}\right)\right]|\phi\rangle \leq 2\sqrt{2} \tag{5.23}$$

$$\langle\phi|\left[Z'_{\mathcal{A}_1}\left(Z_{\mathcal{B}_1}+X_{\mathcal{B}_1}\right)+X'_{\mathcal{A}_1}\left(Z_{\mathcal{B}_1}-X_{\mathcal{B}_1}\right)\right]|\phi\rangle \leq 2\sqrt{2} \tag{5.24}$$

$$\langle\phi|\left[Z_{\mathcal{A}_2}\left(Z_{\mathcal{B}_2}+X_{\mathcal{B}_2}\right)+X_{\mathcal{A}_2}\left(Z_{\mathcal{B}_2}-X_{\mathcal{B}_2}\right)\right]|\phi\rangle \leq 2\sqrt{2} \tag{5.25}$$

$$\langle\phi|\left[Z'_{\mathcal{A}_2}\left(Z_{\mathcal{B}_2}+X_{\mathcal{B}_2}\right)+X'_{\mathcal{A}_2}\left(Z_{\mathcal{B}_2}-X_{\mathcal{B}_2}\right)\right]|\phi\rangle \leq 2\sqrt{2} \tag{5.26}$$

In order to see (5.21) and (5.22) hold, the above inequalities must take the equal sign. Having these equalities, we could now apply the Theorem 4 in Chapter 3 to all of them, and it will allow us to prove the anti-commutativity of the following pairs of operators,

$$\begin{aligned} \{Z_{\mathcal{A}_1},X_{\mathcal{A}_1}\}=0, &\qquad \{Z'_{\mathcal{A}_1},X'_{\mathcal{A}_1}\}=0,\\ \{Z_{\mathcal{A}_2},X_{\mathcal{A}_2}\}=0, &\qquad \{Z'_{\mathcal{A}_2},X'_{\mathcal{A}_2}\}=0,\\ \{V_{\mathcal{B}_1},W_{\mathcal{B}_1}\}=0, &\qquad \{V_{\mathcal{B}_2},W_{\mathcal{B}_2}\}=0, \end{aligned} \tag{5.27}$$

where

$$V_{\mathcal{B}_1} = \frac{Z_{\mathcal{B}_1} + X_{\mathcal{B}_1}}{|Z_{\mathcal{B}_1} + X_{\mathcal{B}_1}|}, \qquad W_{\mathcal{B}_1} = \frac{Z_{\mathcal{B}_1} - X_{\mathcal{B}_1}}{|Z_{\mathcal{B}_1} - X_{\mathcal{B}_1}|}, \tag{5.28}$$

$$V_{\mathcal{B}_2} = \frac{Z_{\mathcal{B}_2} + X_{\mathcal{B}_2}}{|Z_{\mathcal{B}_2} + X_{\mathcal{B}_2}|}, \qquad W_{\mathcal{B}_2} = \frac{Z_{\mathcal{B}_2} - X_{\mathcal{B}_2}}{|Z_{\mathcal{B}_2} - X_{\mathcal{B}_2}|}, \tag{5.29}$$

and $|Z_{\mathcal{B}_1} \pm X_{\mathcal{B}_1}| = |Z_{\mathcal{B}_2} \pm X_{\mathcal{B}_2}| = \sqrt{2}$. Due to the anti-commutativity of V and W, it will also follow that the anti-commutativity of Z and X on B,

$$\{Z_{\mathcal{B}_1}, X_{\mathcal{B}_1}\} = 0, \qquad \{Z_{\mathcal{B}_2}, X_{\mathcal{B}_2}\} = 0. \tag{5.30}$$

In addition, we would get the following relations,

$$Z_{\mathcal{A}_1} |\phi\rangle = W_{\mathcal{B}_1} |\phi\rangle = Z'_{\mathcal{A}_1} |\phi\rangle\,, \tag{5.31}$$

$$X_{\mathcal{A}_1} |\phi\rangle = V_{\mathcal{B}_1} |\phi\rangle = X'_{\mathcal{A}_1} |\phi\rangle\,, \tag{5.32}$$

$$Z_{\mathcal{A}_2} |\phi\rangle = W_{\mathcal{B}_2} |\phi\rangle = Z'_{\mathcal{A}_2} |\phi\rangle\,, \tag{5.33}$$

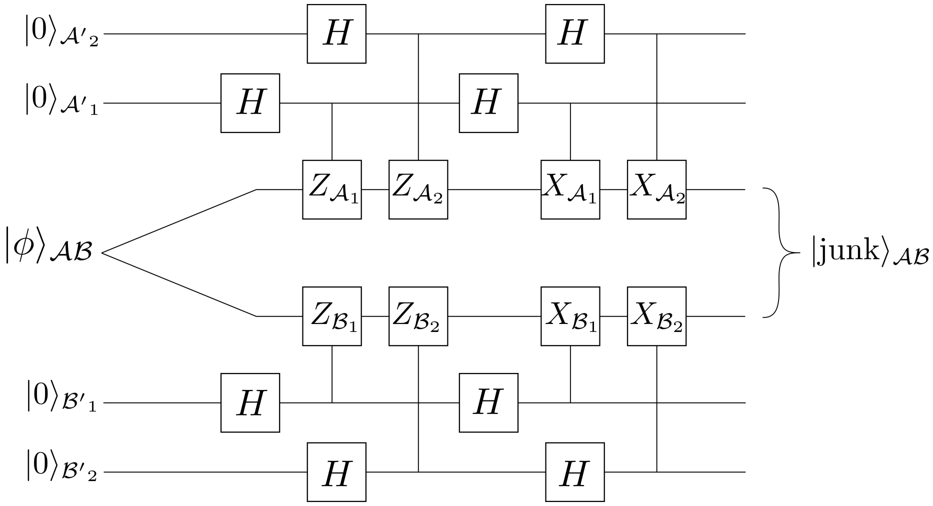
$$X_{\mathcal{A}_2} |\phi\rangle = V_{\mathcal{B}_2} |\phi\rangle = X'_{\mathcal{A}_2} |\phi\rangle\,. \tag{5.34}$$

Similar to (5.20), we could also derive that,

$$\begin{aligned} [X_{\mathcal{B}_1}, X_{\mathcal{B}_2}] &= 0, & [Z_{\mathcal{B}_1}, Z_{\mathcal{B}_2}] &= 0, \\ [Z_{\mathcal{B}_1}, Z_{\mathcal{B}_2}] &= 0, & [X_{\mathcal{B}_1}, X_{\mathcal{B}_2}] &= 0. \end{aligned} \tag{5.35}$$

With all these properties derived above, the isometry in Figure 5.2 will successfully map the state of the system $|\phi\rangle$ into the target state (5.6).

□



$|0\rangle_{\mathcal{A}'_2}$
$|0\rangle_{\mathcal{A}'_1}$
$|\phi\rangle_{\mathcal{AB}}$
$|0\rangle_{\mathcal{B}'_1}$
$|0\rangle_{\mathcal{B}'_2}$
H
$Z_{\mathcal{A}_1}$
$Z_{\mathcal{A}_2}$
$X_{\mathcal{A}_1}$
$X_{\mathcal{A}_2}$
$Z_{\mathcal{B}_1}$
$Z_{\mathcal{B}_2}$
$X_{\mathcal{B}_1}$
$X_{\mathcal{B}_2}$
$|\mathrm{junk}\rangle_{\mathcal{AB}}$

Figure 5.2: Local isometry that extracts the target state from the system into the ancillary qubits. H is the qubit Hadamard gate.

5.1.2 Self-testing with SDP and the robustness bound

Instead of going through the tedious analytical proof of the self-testing, a more simple method would be using the NPA hierarchy and SDP program to test the criterion directly.

Generally speaking, a local operation for two qubits that extract the information out of the system, for example on A, could always be expressed as the following

$$\begin{aligned}\mathcal{S}_{\mathcal{A}\mathcal{A}'}\left|00\right\rangle_{\mathcal{A}'} = &\left|00\right\rangle_{\mathcal{A}'} \pi^{\mathcal{A}_1}_{z=0}\pi^{\mathcal{A}_2}_{z=0}\\ &+ \left|01\right\rangle_{\mathcal{A}'} \sigma^{\mathcal{A}_2}_x\, \pi^{\mathcal{A}_1}_{z=0}\pi^{\mathcal{A}_2}_{z=1}\\ &+ \left|10\right\rangle_{\mathcal{A}'} \sigma^{\mathcal{A}_1}_x\, \pi^{\mathcal{A}_1}_{z=1}\pi^{\mathcal{A}_2}_{z=0}\\ &+ \left|11\right\rangle_{\mathcal{A}'} \sigma^{\mathcal{A}_1}_x\sigma^{\mathcal{A}_2}_x\, \pi^{\mathcal{A}_1}_{z=1}\pi^{\mathcal{A}_2}_{z=1},\end{aligned} \tag{5.36}$$

where σ_x and π_z are the ideal Pauli-x operation and projector of the Pauli-z operation on the ideal subspaces. However, when we are dealing with the case where the two subsystems are considered as a whole, normally we do not have information of the behaviour of the subsystems. Inspired from the ideal strategy (5.7), a possible proposal for the realizations of the above operations on each subsystem would be

$$\begin{aligned}
\pi^{\mathcal{A}_1}_{z=s}\pi^{\mathcal{A}_2}_{z=t} &\longrightarrow \Pi_{2s+t|0}\,, \\
\sigma_x^{\mathcal{A}_1} &\longrightarrow \Pi_{0|3}+\Pi_{1|3}-\Pi_{2|3}-\Pi_{3|3}\,, \\
\sigma_x^{\mathcal{A}_2} &\longrightarrow \Pi_{0|3}-\Pi_{1|3}+\Pi_{2|3}-\Pi_{3|3}\,, \\
\sigma_x^{\mathcal{A}_1}\,\sigma_x^{\mathcal{A}_2} &\longrightarrow \Pi_{0|3}-\Pi_{1|3}-\Pi_{2|3}+\Pi_{3|3}\,.
\end{aligned} \tag{5.37}$$

Thus, the local isometry for A will be expressed as

$$\begin{aligned}
\mathcal{S}_{\mathcal{A}\mathcal{A}'}\left|00\right\rangle_{\mathcal{A}'} = &\left|00\right\rangle_{\mathcal{A}'}\Pi_{0|0} \\
&+\left|01\right\rangle_{\mathcal{A}'}\left(\Pi_{0|3}-\Pi_{1|3}+\Pi_{2|3}-\Pi_{3|3}\right)\Pi_{1|0} \\
&+\left|10\right\rangle_{\mathcal{A}'}\left(\Pi_{0|3}+\Pi_{1|3}-\Pi_{2|3}-\Pi_{3|3}\right)\Pi_{2|0} \\
&+\left|11\right\rangle_{\mathcal{A}'}\left(\Pi_{0|3}-\Pi_{1|3}-\Pi_{2|3}+\Pi_{3|3}\right)\Pi_{3|0}\,.
\end{aligned} \tag{5.38}$$

In order to check the validity of the above definition of the isometry, we still need to verify whether it is unitary or not.

Proof of (5.38) *to be unitary.* Here we prove that the map

$$\left|\phi\right\rangle_{\mathcal{A}} \longrightarrow \mathcal{S}_{\mathcal{A}\mathcal{A}'}\left|\phi\right\rangle_{\mathcal{A}}\otimes\left|0,0\right\rangle_{\mathcal{A}'}$$

with $\mathcal{S}_{\mathcal{A}\mathcal{A}'}$ satisfying Eq. (5.38) preserves the scalar product. To start, we note that the action of this map can be written as

$$\mathcal{S}_{\mathcal{A}\mathcal{A}'}\left|\phi\right\rangle_{\mathcal{A}}\otimes\left|0,0\right\rangle_{\mathcal{A}'} = \sum_{i,j=0}^{1}\left(S^{i,j}_{\mathcal{A}}\otimes\mathbb{1}\right)\left|\phi\right\rangle_{\mathcal{A}}\otimes\left|i,j\right\rangle_{\mathcal{A}'}\,, \tag{5.39}$$

where $S^{i,j}_{\mathcal{A}}$ are operators acting on Alice's system, which are described in Eq. (5.38), i.e.

$$\begin{aligned}
S^{0,0}_{\mathcal{A}} &= \Pi_{0|0} \\
S^{0,1}_{\mathcal{A}} &= (\Pi_{0|3} - \Pi_{1|3} + \Pi_{2|3} - \Pi_{3|3})\,\Pi_{1|0} \\
S^{1,0}_{\mathcal{A}} &= (\Pi_{0|3} + \Pi_{1|3} - \Pi_{2|3} - \Pi_{3|3})\,\Pi_{2|0} \\
S^{1,1}_{\mathcal{A}} &= (\Pi_{0|3} - \Pi_{1|3} - \Pi_{2|3} + \Pi_{3|3})\,\Pi_{3|0}
\end{aligned} \tag{5.40}$$

The scalar product $\langle \phi' | \phi \rangle_{\mathcal{A}}$, thus becomes

$$\begin{aligned}
&\langle \phi' |_{\mathcal{A}} \otimes \langle 0, 0|_{\mathcal{A}'} \,(S_{\mathcal{A}\mathcal{A}'})^{\dagger}\; S_{\mathcal{A}\mathcal{A}'} \, |\phi\rangle_{\mathcal{A}} \otimes |0,0\rangle_{\mathcal{A}'} \\
&= \sum_{i,j} \langle \phi' |_{\mathcal{A}} \otimes \langle i, j|_{\mathcal{A}'} \,(S^{i,j}_{\mathcal{A}} \otimes \mathbb{1})^{\dagger} \\
&\quad \times \sum_{k,\ell} (S^{k,\ell}_{\mathcal{A}} \otimes \mathbb{1}) \, |\phi\rangle_{\mathcal{A}} \otimes |k,\ell\rangle_{\mathcal{A}'} \\
&= \langle \phi' |_{\mathcal{A}} \; \sum_{i,j} (S^{i,j}_{\mathcal{A}})^{\dagger} \; S^{i,j}_{\mathcal{A}} \;\; |\phi\rangle_{\mathcal{A}} \\
&= \langle \phi | \phi' \rangle_{\mathcal{A}} \,,
\end{aligned} \tag{5.41}$$

where in the last step we used the identity $\sum_{i,j} (S^{i,j}_{\mathcal{A}})^{\dagger} S^{i,j}_{\mathcal{A}} = \mathbb{1}$, which can be checked explicitly. □

If we combine the isometry for B, we will get the isometry that is intended to extract the target state

$$\Psi = \mathcal{S}_{\mathcal{A}\mathcal{A}'} \otimes \mathcal{S}_{\mathcal{B}\mathcal{B}'}. \tag{5.42}$$

Thus, the formalism of SDP will be

$$\begin{aligned}
&\min && F(S) \\
&\text{such that} && |\langle \phi | \, \Pi^{A}_{a|x} \Pi^{B}_{b|y} \, |\phi\rangle - \tilde{p}(ab|xy)| \leq \varepsilon, \\
& && \Gamma(S) \geq 0,
\end{aligned} \tag{5.43}$$

where $\tilde{p}$ is the probability distribution from the ideal strategy, and we choose the sequence S to be,

$$S = \{\mathbb{1}, \Pi_{a|x}, \Pi_{b|y}, \Pi_{a|x}\Pi_{b|y}, \Pi_{a|x=0}\Pi_{a'|x=3}\Pi_{b|y=0}, \Pi_{a|x=0}\Pi_{b|y=3}\Pi_{b'|y=0}\}. \tag{5.44}$$

The robustness bound is given in Figure 5.3

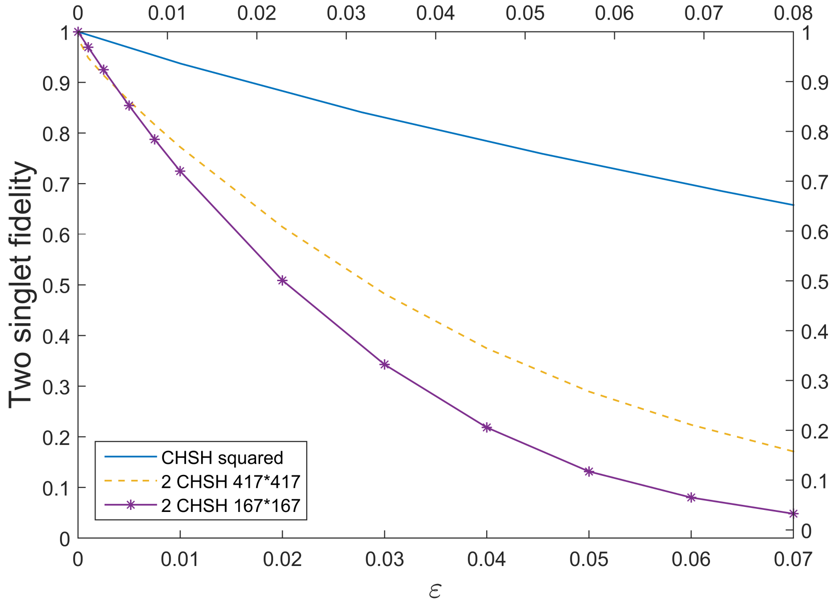


Figure 5.3: Robustness bound of two singlet fidelity as a function of ε. The two lines labelled as 417 × 417 and 167 × 167 correspond to different sequence S, the latter one only includes $\Pi_{a|0}$ and $\Pi_{b|0}$ instead of all the $\Pi_{a|x}$ and $\Pi_{b|y}$. As a comparison, we also plot the square of the singlet self-testing fidelity, which is a fair estimation of the sequential CHSH test on two singlets.

Compared to the work of RUV [45, 94], our robustness managed to make a dramatic improve.[1] This value of the fidelity is not yet of practical interest. However, if we are not tied to loophole-free experiment, the state of art violation of the CHSH inequality is $B_{CHSH} = 2.8276$ [100]. This will give $\varepsilon = 3 \times 10^4$, for which our SDP certifies $F_1 \geq 0.999$ and $F \geq 0.996$.

5.2 Parallel self-testing of two singlet states using Magic Square Box game

As we have seen, the two singlet states can actually be self-tested with the statistics arising from the ideal strategy of two CHSH test. Besides the CHSH, the magic square game is also well known for its weirdness and the optimality associated to singlet states. This makes us to come up with the idea of self-testing two singlet states using magic square game.

We will give a short review of the magic square game [101, 102, 103]. Suppose each of A and B has a box which has nine bulbs on it, as in Figure 5.4. Each bulb could have two possible colours and each column or row is associated with a button on the boxes. When the game is played, A will choose the buttons that decides which one of the three rows is going to light on, and B will choose the buttons that decides which one of the three columns is going to light on.

The winning criterion of A and B is:

1. The intersection bulbs of A and B always have the same colour,

2. Whichever column or row is chosen, the number of red bulbs is always even except the third column of B.

It is shown in [103] that, to win the game, A and B could perform the following

[1] In Eq. (41) of [32] we find the estimate $||\psi - \bar{\psi} \otimes |\text{junk}\rangle||^2 \leq 72284 \times 4\varepsilon$ (notice that ε in that paper is equal to $2\sqrt{2}\varepsilon$ in our notation). Even leaving self-testing aside, the algebraic maximum of the l.h.s. is 2; therefore the estimate is trivial for $\varepsilon \geq \frac{1}{144568}$.

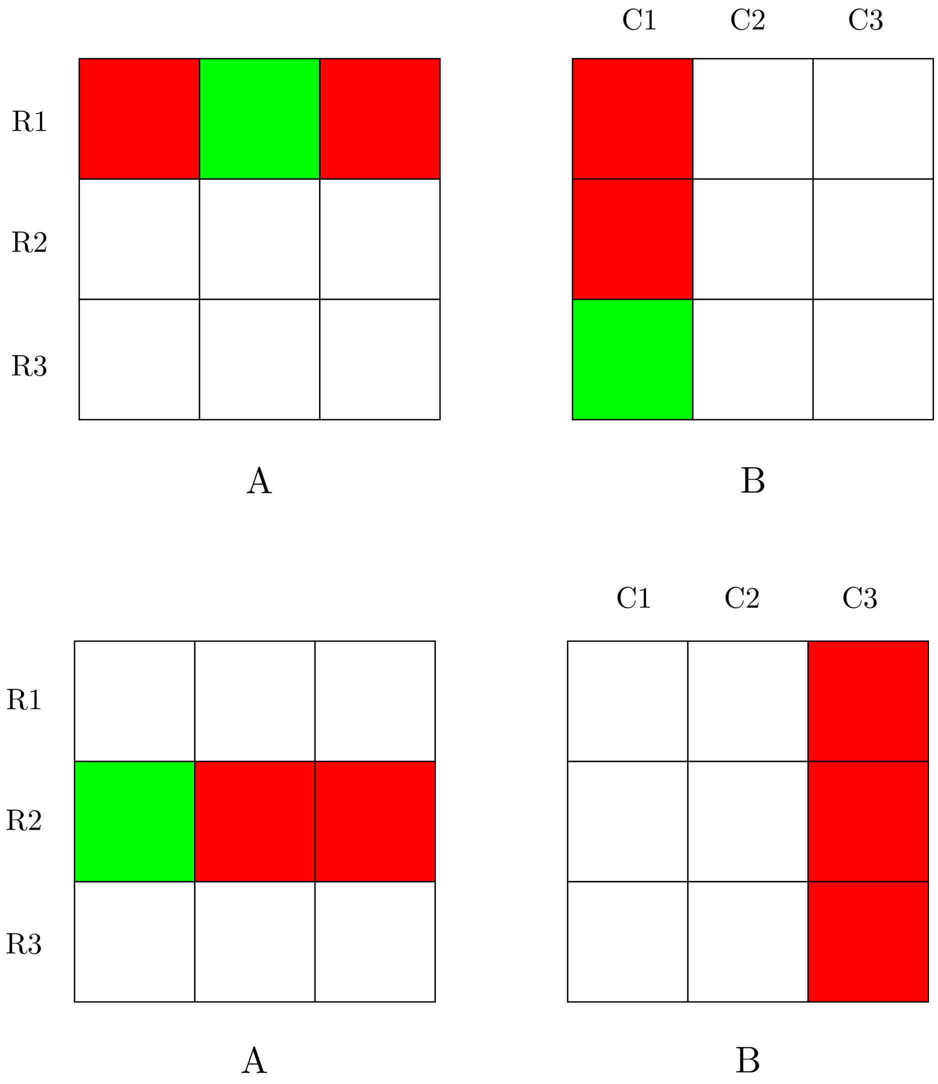


Figure 5.4: Examples of the results that satisfy the winning criterion.

measurements on two singlet states

$$|\phi\rangle = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes 2}. \tag{5.45}$$

The measurements corresponding to the buttons of R1, R2, R3 are $\sigma_z \otimes \sigma_z$, $\sigma_x \otimes \sigma_x$ and $\sigma_y \otimes \sigma_y$. With such three measurements, A could recover all the colours of the three bulbs in each row he choose. Similarly,the measurements corresponding to the buttons of C1, C2, C3 are $\sigma_x \otimes \sigma_z$, $\sigma_z \otimes \sigma_x$ and $\sigma_y \otimes \sigma_y$, see Table 5.1.

	C1	C2	C3
R1	$\sigma_z \otimes \mathbb{1}$	$\mathbb{1} \otimes \sigma_z$	$\sigma_z \otimes \sigma_z$
R2	$\mathbb{1} \otimes \sigma_x$	$\sigma_x \otimes \mathbb{1}$	$\sigma_x \otimes \sigma_x$
R3	$\sigma_z \otimes \sigma_x$	$\sigma_x \otimes \sigma_z$	$\sigma_y \otimes \sigma_y$

Table 5.1: Measurement strategy to win the magic square game.

In the following, we are going to try to use the statistics that is achieved with the above strategy as a criterion to self-test two singlet states.

An analytical proof of the self-testing will be found in [104]. For simplicity, we will just introduce the SDP method to self-test the state here.

Before going into the details about the SDP method, we will first make a small simplification of the original problem. If we apply a rotation $R_y(\pi/2)$ on the second qubit of B, we will be able to transform the original strategy into the following measurements

$$\text{R1/C1:} \quad \{\pi_z \otimes \pi_z\}, \quad \text{R2/C2:} \quad \{\pi_x \otimes \pi_x\}, \quad \text{R3/C3:} \quad \{|\chi_\pm\rangle\langle\chi_\pm|, |\chi'_\pm\rangle\langle\chi'_\pm|\} \tag{5.46}$$

on the state

$$|\phi\rangle = \frac{|00\rangle_{\mathcal{A}_1\mathcal{B}_1} + |11\rangle_{\mathcal{A}_1\mathcal{B}_1}}{\sqrt{2}} \otimes \frac{(|00\rangle + |11\rangle)_{\mathcal{A}_2\mathcal{B}_2} + (|01\rangle - |10\rangle)_{\mathcal{A}_2\mathcal{B}_2}}{2}, \tag{5.47}$$

where $|\chi_\pm\rangle = \big((|00\rangle - |11\rangle)_{\mathcal{A}_2\mathcal{B}_2} + (|01\rangle + |10\rangle)_{\mathcal{A}_2\mathcal{B}_2}\big)/2$ and $|\chi'_\pm\rangle = \big((|00\rangle + |11\rangle)_{\mathcal{A}_2\mathcal{B}_2} + (|01\rangle - |10\rangle)_{\mathcal{A}_2\mathcal{B}_2}\big)/2$.

Now we can consider how to construct the isometry which is necessary for the SDP. Comparing with the formalism of the two qubits isometry in (5.36) and (5.38), we found that, the problem we are encountering here is in fact quite similar to it. The isometry is indeed the same as the one in the double CHSH case, since the ideal measurements on R1/C1 and R2/C2 are the same as that of $A_{0/3}$ and $B_{0/3}$ of the double CHSH case.

Thus, the local isometry for A will be expressed as

$$\begin{aligned}\mathcal{S}_{\mathcal{A}\mathcal{A}'}\left|00\right\rangle_{\mathcal{A}'} = &\left|00\right\rangle_{\mathcal{A}'}\Pi_{0|1}\\ &+\left|01\right\rangle_{\mathcal{A}'}\left(\Pi_{0|2}-\Pi_{1|2}+\Pi_{2|2}-\Pi_{3|2}\right)\Pi_{1|0}\\ &+\left|10\right\rangle_{\mathcal{A}'}\left(\Pi_{0|2}+\Pi_{1|2}-\Pi_{2|2}-\Pi_{3|2}\right)\Pi_{2|0}\\ &+\left|11\right\rangle_{\mathcal{A}'}\left(\Pi_{0|2}-\Pi_{1|2}-\Pi_{2|2}+\Pi_{3|2}\right)\Pi_{3|0}\,,\end{aligned} \tag{5.48}$$

where we use $\Pi_{a|r}$ to denote the projector for the outcome a with respect to the button R_r pressed, similar for B. As we proved before, this is a valid isometry in the sense that it is unitary for arbitrary input state. If we combine the isometry for B, we will get the isometry that is intended to extract the target state

$$\Psi = \mathcal{S}_{\mathcal{A}\mathcal{A}'}\otimes\mathcal{S}_{\mathcal{B}\mathcal{B}'}. \tag{5.49}$$

Thus, the formalism of SDP will be

$$\begin{aligned}\min\quad & F(S)\\ \text{such that}\quad & \left|\left\langle\phi\right|\Pi^{A}_{a|r}\Pi^{B}_{b|c}\left|\phi\right\rangle-\tilde{p}(ab|rc)\right|\leq\varepsilon,\\ & \Gamma(S)\geq 0,\end{aligned} \tag{5.50}$$

where $\tilde{p}$ is the probability distribution from the ideal strategy, and we choose the sequence S to be,

$$S=\{\mathbb{1},\Pi_{a|r},\Pi_{b|c},\Pi_{a|r}\Pi_{b|c},\Pi_{a|r=1}\Pi_{a'|r=2}\Pi_{b|c=1},\Pi_{a|r=1}\Pi_{b|c=2}\Pi_{b'|c=1}\}. \tag{5.51}$$

The robustness bound is given in Figure 5.5.

As we could see, the robustness converges to one when the error in the statistics

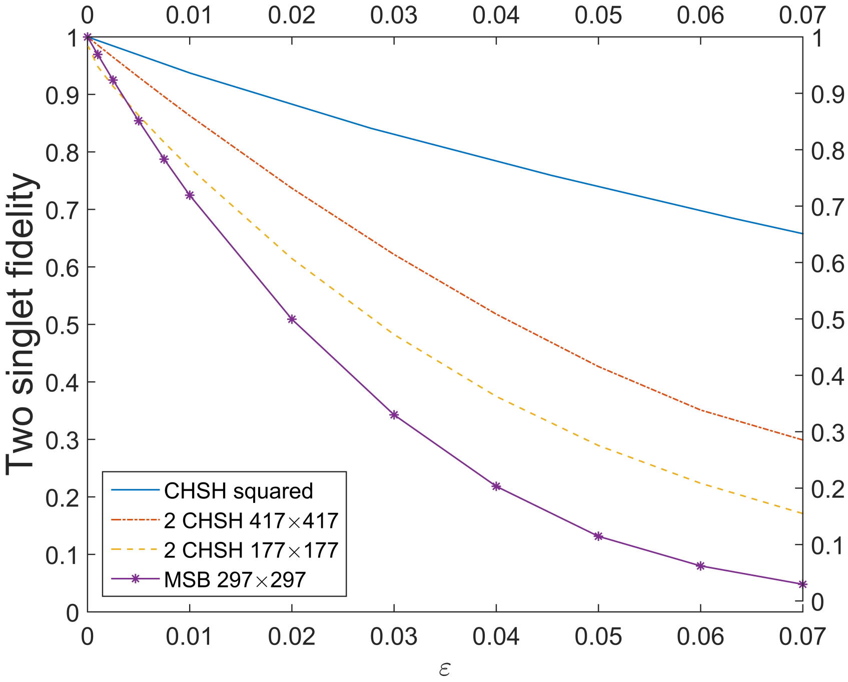


Figure 5.5: Robustness bound of two singlet fidelity as a function of ε. The two lines labelled as 417×417 and 167×167 correspond to different sequence S. As a comparison, we also plot the square of the singlet self-testing fidelity.

is zero, which simply indicates the self-testing in the ideal case works.

From the comparison to the double CHSH test, the Magic Square criterion seems to be less robust. Even comparing with the bound of the double CHSH test that uses a smaller matrix and similar imperfect resources. The results also suggest that the parallel self-testing is different from two independent copies. However, it should be reminded that definite and general comparisons cannot be drawn, since the bounds are not guaranteed to be tight absolutely.

5.3 Parallel self-testing of N singlet states?

From the result we have shown above, we could see that a parallel self-testing of two singlet states are actually possible. This motivates us to ask whether a generalization of the method to N pairs of singlet states will still work. Due to the limitation of the computational power, it could not be checked directly by SDP methods. However, recent results that generalize our methods show that it is possible to self-test with both N CHSH test [105] and generalized magic square game for N pair of singlets [106].

Chapter 6

Conclusion

In this thesis, we discussed a variety of topics related to self-testing, a device independent way that characterizes the quantum systems.

We started by introducing the basics of quantum nonlocality and the idea of polytopes for local set. Regarding the quantum set, we introduced the NPA hierarchy [11] characterization and took its advantage to apply to the problems of self-testing.

In the study of the bipartite self-testing, we stepped further comparing the original study of the limit examples of states in the literatures. Specifically, we managed to show all the criteria that self-test the singlet state. With the generalization to partially entangled state, we recovered all the extremal points of the quantum set in the bipartite qubit scenario and proved that all of them actually self-test the partially entangled state. Along with the by-products of the SDP methods, we are able to know more about the properties of the quantum set at the boundary points, explicitly we have shown that the extremal point in this case does not lie in a surface of dimension seven, one less than the dimension of the quantum set, but actually resides in an even lower dimensional subspace in the whole quantum set.

Later, we study the self-testing of multi-partite systems. We managed to show that all the 3-qubit state with real coefficients can actually be self-tested and a specific class of N qubit state, namely the N-qubit W state could also be self-tested.

Lastly, we give explicit examples of criteria that self-test two singlet states in parallel and the robustness of the methods is applicable regarding the state of art of current experiments. This work has brought a lot interests to the field of computer science that many of those results coming out recently actually share similar ideas as ours [107, 106, 105, 108, 109, 110]. Our results have been generalized to N pairs with both the parallel CHSH test and Magic Square game we studied. This is essential to the well known quantum computing scheme proposed by [45, 94].

Through the study in this thesis, we are able to use the idea of self-testing to not only study the device independent certification of unknown devices and enrich the scenarios that could be self-tested by studying a variety of states, but also utilize it as a tool to study the boundary properties of the quantum set. Even though, it is now limited to the bipartite qubit case, it give us an opportunity to unveil the long lasting mystery of the quantum boundaries, and we hope more investigation could be made to more scenarios.

We are also looking forward to seeing more examples of self-testing to enrich the zoo, especially, whether an entangled state with arbitrary number of parties in arbitrary dimensions could be self-tested? Is it possible to self-test a quantum state with phase involved? Concerning the robustness, with the recent new technique [58], whether it is possible to generalize it to more states other than the 2-qubit singlet state? In terms of the self-testing itself, with the standard formalism always involving ancillary qubits, which is believed to give more power to self-testing [111, 112], whether it is possible to get rid of these ancillas and even open the ”black box” to play directly with the device itself? Hopefully, with these questions answered, we can bring our knowledge about self-testing to a new level.

Appendix A

Analytical robustness bound for W state self-testing

This appendix provides the details of the derivation of the analytical bound (4.32).

We first introduce the following lemma:

Proposition 2. *Suppose each statistics in (4.3), (4.4) and (4.5), in the order of appearance, has a deviation $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{15}$ from its expected value, e.g.*

$$\langle\phi| \Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{1|0} |\phi\rangle = \frac{1}{3} + \varepsilon_1, \tag{A.1}$$

for the first term, then,

$$\begin{cases} \|(\Pi^A_{0|0}B_1B_0 + \Pi^A_{0|0}B_0B_1)|\phi\rangle\| \leq \delta_1 \\ \|(\Pi^A_{0|0}B_0C_0 + \Pi^A_{0|0}C_0C_1)|\phi\rangle\| \leq \delta_2 \\ \|(\Pi^A_{0|0}B_1 - \Pi^A_{0|0}C_1)|\phi\rangle\| \leq \delta_3 \\ \|(\Pi^A_{0|0}B_0 + \Pi^A_{0|0}C_0)|\phi\rangle\| \leq \delta_4, \end{cases} \tag{A.2}$$

(A.3)

$$\begin{cases} \|(\Pi^B_{0|0}A_1A_0 + \Pi^B_{0|0}A_0A_1)\,|\phi\rangle\,\| \le \delta_5 \\ \|(\Pi^B_{0|0}C_1C_0 + \Pi^B_{0|0}C_0C_1)\,|\phi\rangle\,\| \le \delta_6 \\ \|(\Pi^B_{0|0}A_1 - \Pi^B_{0|0}C_1)\,|\phi\rangle\,\| \le \delta_7 \\ \|(\Pi^B_{0|0}A_0 + \Pi^B_{0|0}C_0)\,|\phi\rangle\,\| \le \delta_8, \end{cases} \tag{A.4}$$

where δ_is are functions of ε_is.

Proof. We give the proof for (A.2), the proof for (A.4) is similar.

To be rigorous, we assume

$$\begin{aligned} \langle\phi|\,\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\,|\phi\rangle &= \varepsilon_{16} \\ \langle\phi|\,\Pi^A_{0|0}\Pi^B_{1|0}\Pi^C_{1|0}\,|\phi\rangle &= \varepsilon_{17} \\ \langle\phi|\,\Pi^A_{1|0}\Pi^B_{0|0}\Pi^C_{1|0}\,|\phi\rangle &= \varepsilon_{18} \\ \langle\phi|\,\Pi^A_{1|0}\Pi^B_{1|0}\Pi^C_{0|0}\,|\phi\rangle &= \varepsilon_{19} \\ \langle\phi|\,\Pi^A_{1|0}\Pi^B_{1|0}\Pi^C_{1|0}\,|\phi\rangle &= \varepsilon_{20}. \end{aligned} \tag{A.5}$$

We can now write

$$\begin{aligned} \|\Pi^A_{0|0}B_1\,|\phi\rangle\,\| &= \sqrt{|\,\langle\phi|\,\Pi^A_{0|0}B_1B_1\Pi^A_{0|0}\,|\phi\rangle\,|} \\ &= \sqrt{|\,\langle\phi|\,(\Pi^A_{0|0})^2\,|\phi\rangle\,|} = \sqrt{|\,\langle\phi|\,\Pi^A_{0|0}\,|\phi\rangle\,|} \\ &= \sqrt{\frac{2}{3} - (\varepsilon_1 + \varepsilon_2 + \varepsilon_{16} + \varepsilon_{17})} \\ &= \sqrt{\frac{2}{3} - \delta_0}. \end{aligned} \tag{A.6}$$

where $\delta_0 = \varepsilon_1 + \varepsilon_2 + \varepsilon_{16} + \varepsilon_{17}$ and they all come from results which involve $\Pi^A_{0|0}$.

Similarly,

$$\begin{aligned}
&\|\Pi^A_{0|0}B_0 \ket{\phi}\| = \|\Pi^A_{0|0}C_1 \ket{\phi}\| = \|\Pi^A_{0|0}C_0 \ket{\phi}\| \\
&= \|\Pi^A_{0|0}C_2 \ket{\phi}\| = \sqrt{\frac{2}{3} - \delta_0}.
\end{aligned} \tag{A.7}$$

Then,

$$\begin{aligned}
&\|(\Pi^A_{0|0}B_1 - \Pi^A_{0|0}C_1)\ket{\phi}\| \\
&= \sqrt{|\bra{\phi}\Pi^A_{0|0}B_1B_1\Pi^A_{0|0} + \Pi^A_{0|0}C_1C_1\Pi^A_{0|0} - 2\Pi^A_{0|0}B_1C_1\Pi^A_{0|0}\ket{\phi}|} \\
&= \sqrt{\begin{aligned}&|\bra{\phi}\Pi^A_{0|0}B_1B_1\Pi^A_{0|0}\ket{\phi} + \bra{\phi}\Pi^A_{0|0}C_1C_1\Pi^A_{0|0}\ket{\phi} \\ &- 2\bra{\phi}\Pi^A_{0|0}B_1C_1\Pi^A_{0|0}\ket{\phi}|\end{aligned}} \\
&= \sqrt{|(\frac{2}{3} - \delta_0) \times 2 - 2 \times (\frac{2}{3} - \varepsilon_5)|} \\
&= \sqrt{2|\delta_0 - \varepsilon_5|}.
\end{aligned} \tag{A.8}$$

Using the same techniques, we are able to get

$$\|(\Pi^A_{0|0}B_0 - \Pi^A_{0|0}C_0)\ket{\phi}\| = \sqrt{2|\delta_0 - \varepsilon_4|}. \tag{A.9}$$

To get the first line of (A.2), we estimate the following distance,

$$\begin{aligned}
&\|(\Pi^A_{0|0}C_2 - \frac{\Pi^A_{0|0}B_1 - \Pi^A_{0|0}B_0}{\sqrt{2}}) |\phi\rangle \| \\
&= \sqrt{\begin{aligned} &| \langle\phi| \Pi^A_{0|0}C_2C_2\Pi^A_{0|0} + \frac{1}{2}\Pi^A_{0|0}B_1B_1\Pi^A_{0|0} \\ &+ \frac{1}{2}\Pi^A_{0|0}B_0B_0\Pi^A_{0|0} - \Pi^A_{0|0}B_1B_0\Pi^A_{0|0} \\ &- \sqrt{2}\Pi^A_{0|0}C_2B_1\Pi^A_{0|0} + \sqrt{2}\Pi^A_{0|0}C_2B_0\Pi^A_{0|0} |\phi\rangle |\end{aligned}} \\
&= \sqrt{\begin{aligned} &|(\frac{2}{3} - \delta_0) \times 2 - \sqrt{2} \times (\frac{1}{\sqrt{2}}\frac{2}{3} - \varepsilon_8) \\ &- \sqrt{2} \times (\frac{1}{\sqrt{2}}\frac{2}{3} - \varepsilon_9) - \langle\phi| \Pi^A_{0|0}B_1B_0 |\phi\rangle |\end{aligned}} \\
&= \sqrt{|\sqrt{2}(\sqrt{2}\delta_0 - \varepsilon_8 - \varepsilon_9) + \langle\phi| \Pi^A_{0|0}B_1B_0 |\phi\rangle |} \\
&\leq \sqrt{\begin{aligned} &|\sqrt{2}(\sqrt{2}\delta_0 - \varepsilon_8 - \varepsilon_9)| + |\varepsilon_6| \\ &+ \sqrt{\frac{2}{3} - \delta_0} \times \sqrt{|2(\delta_0 - \varepsilon_4)|}\end{aligned}} \\
&= \frac{\delta_1}{(2 + 2\sqrt{2})\sqrt{2}},
\end{aligned} \tag{A.10}$$

where the $| \langle\phi| \Pi^A_{0|0}B_1B_0 |\phi\rangle |$ is estimated by using the triangle inequality $|a + b| \leq |a| + |b|$ and Cauchy–Schwarz inequality $|a \cdot b| \leq |a| \cdot |b|$,

$$\begin{aligned}
&| \langle\phi| \Pi^A_{0|0}B_1B_0 |\phi\rangle | = | \langle\phi| \Pi^A_{0|0}B_1(C_0 + B_0 - C_0) |\phi\rangle | \\
&\leq | \langle\phi| \Pi^A_{0|0}B_1C_0 |\phi\rangle | + | \langle\phi| \Pi^A_{0|0}B_1(B_0 - C_0) |\phi\rangle | \\
&= |\varepsilon_6| + | \langle\phi| \Pi^A_{0|0}B_1(B_0 - C_0) |\phi\rangle | \\
&\leq |\varepsilon_6| + \|\Pi^A_{0|0}B_1 |\phi\rangle \| \cdot \|(B_0 - C_0) |\phi\rangle \| \\
&= |\varepsilon_6| + \sqrt{\frac{2}{3} - \delta_0} \times \sqrt{|2(\delta_0 - \varepsilon_4)|}.
\end{aligned} \tag{A.11}$$

In order to estimate the $\|(\Pi^A_{0|0}B_1B_0+\Pi^A_{0|0}B_0B_1)\left|\phi\right\rangle\|$, first consider,

$$\begin{aligned}
&(\Pi^A_{0|0}C_2)^2\left|\phi\right\rangle\\
&=(\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}}+\Pi^A_{0|0}C_2-\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})^2\left|\phi\right\rangle\\
&=(\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})^2\left|\phi\right\rangle\\
&+(\Pi^A_{0|0}C_2-\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})^2\left|\phi\right\rangle\\
&+2(\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})(\Pi^A_{0|0}C_2-\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})\left|\phi\right\rangle.
\end{aligned}\tag{A.12}$$

The first term contains the anticommutative terms while the last two terms have a same factor. By using the identity $C_2^2\left|\phi\right\rangle=B_1^2\left|\phi\right\rangle=B_0^2\left|\phi\right\rangle=\left|\phi\right\rangle$, we can easily deduce that,

$$\begin{aligned}
&\frac{(\Pi^A_{0|0}B_1B_0+\Pi^A_{0|0}B_0B_1)\left|\phi\right\rangle}{\sqrt{2}}\\
=&(\Pi^A_{0|0}C_2+\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})\\
&(\Pi^A_{0|0}C_2-\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})\left|\phi\right\rangle,
\end{aligned}\tag{A.13}$$

and the norm can be estimated,

$$\begin{aligned}
&\|\frac{(\Pi^A_{0|0}B_1B_0+\Pi^A_{0|0}B_0B_1)\left|\phi\right\rangle}{\sqrt{2}}\|\\
&\leq\|\Pi^A_{0|0}C_2(\Pi^A_{0|0}C_2-\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})\left|\phi\right\rangle\|\\
&+\frac{1}{\sqrt{2}}\|\Pi^A_{0|0}B_1(\Pi^A_{0|0}C_2-\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})\left|\phi\right\rangle\|\\
&+\frac{1}{\sqrt{2}}\|\Pi^A_{0|0}B_0(\Pi^A_{0|0}C_2-\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})\left|\phi\right\rangle\|\\
&\leq(\|\Pi^A_{0|0}C_2\|_\infty+\frac{1}{\sqrt{2}}\|\Pi^A_{0|0}B_1\|_\infty+\frac{1}{\sqrt{2}}\|\Pi^A_{0|0}B_0\|_\infty)\\
&\times\|(\Pi^A_{0|0}C_2-\frac{\Pi^A_{0|0}B_1-\Pi^A_{0|0}B_0}{\sqrt{2}})\left|\phi\right\rangle\|.
\end{aligned}\tag{A.14}$$

The infinite norm can be estimated

$$
\begin{aligned}
&\|\Pi^A_{0|0}C_2\|_\infty \leq \|\Pi^A_{0|0}\|_\infty\|C_2\|_\infty \\
&= \|\Pi^A_{0|0}\|_\infty\|P^0_D - P^1_D\|_\infty \leq \|\Pi^A_{0|0}\|_\infty(\|P^0_D\|_\infty + \|P^1_D\|_\infty) \\
&= 2. \qquad (A.15)
\end{aligned}
$$

Similar for $\|\Pi^A_{0|0}B_0\|_\infty$ and $\|\Pi^A_{0|0}B_1\|_\infty$. Then, we get

$$
\|\frac{(\Pi^A_{0|0}B_1B_0 + \Pi^A_{0|0}B_0B_1)\,|\phi\rangle}{\sqrt{2}}\| \leq \frac{\delta_1}{\sqrt{2}}. \qquad (A.16)
$$

The other relations can be proved similarly. □

Using the above proposition, we can now turn into the robustness of the W_3 state. We shall use the isometry with the same local operations described in Figure (2.1), irrespective of the errors in the statistics. The output state can always be displayed as (4.24), the problem then is whether we can prove it's close to the target state $|\text{junk}\rangle_{\mathcal{ABC}}\,|W_3\rangle_{\mathcal{A'B'C'}}$. However, it's not easy to figure out what is the exact form of this target state. What we want to do first is to estimate the distance

$$
\|\Psi(|\phi\rangle_{\mathcal{ABC}} \otimes |000\rangle_{\mathcal{A'B'C'}}) - \sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\,|\phi\rangle_{\mathcal{ABC}} \otimes |W_3\rangle_{\mathcal{A'B'C'}}\|. \qquad (A.17)
$$

There would be 8 terms regarding to the ancillary qubits. We need to estimate the norm of each term. Since there are too many terms involved, we shall only show explicitly some of them, for instance the term

$$
\begin{aligned}
&\|\Pi^A_{0|0}\Pi^B_{0|0}C_1\Pi^C_{1|0}\,|\phi\rangle\,|001\rangle \\
&- \Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}C_1\,|\phi\rangle\,|001\rangle\,\| \\
&= \|\Pi^A_{0|0}\Pi^B_{0|0}C_1\Pi^C_{1|0}\,|\phi\rangle\,|001\rangle - \Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}C_1\,|\phi\rangle\,|001\rangle\,\|. \qquad (A.18)
\end{aligned}
$$

From Proposition 2, we could see that the operator pairs $\{A_0, A_1\}$, $\{B_0, B_1\}$ and $\{C_0, C_1\}$ are almost anticommutative. Thus, the operators $\{A_0, A_1\}$, $\{B_0, B_1\}$ and

$\{C_0, C_1\}$ in (4.24) other than $|001\rangle$, $|010\rangle$ and $|100\rangle$ can always be moved to the right of $\Pi_{1|0}^{A/B/C}$ with the cost of a small error. Using (A.4), we have,

$$\begin{aligned}
&\|\Pi_{0|0}^{A}\Pi_{0|0}^{B}C_1\Pi_{1|0}^{C}|\phi\rangle|001\rangle - \Pi_{0|0}^{A}\Pi_{0|0}^{B}\Pi_{0|0}^{C}C_1|\phi\rangle|001\rangle\| \\
=&\|\Pi_{0|0}^{A}\Pi_{0|0}^{B}C_1C_0|\phi\rangle|001\rangle + \Pi_{0|0}^{A}\Pi_{0|0}^{B}C_0C_1|\phi\rangle|001\rangle\| \\
\leq&\|\Pi_{0|0}^{B}\|_\infty\|\Pi_{0|0}^{A}C_1C_0|\phi\rangle|001\rangle + \Pi_{0|0}^{A}C_0C_1|\phi\rangle|001\rangle\| \\
=&\delta_1.
\end{aligned} \tag{A.19}$$

Similarly, the terms with $|010\rangle$ and $|100\rangle$ can also be shown to be bounded by the same errors. For the other 5 terms in (4.24), by using the properties $A_1^2 = B_1^2 = C_1^2 = 1$, it shows that,

$$\begin{aligned}
&\|\Pi_{0|0}^{A}\Pi_{0|0}^{B}\Pi_{0|0}^{C}|\phi\rangle|000\rangle + \Pi_{0|0}^{A}B_1\Pi_{1|0}^{B}C_1\Pi_{1|0}^{C}|\phi\rangle|011\rangle \\
&+ A_1\Pi_{1|0}^{A}\Pi_{0|0}^{B}C_1\Pi_{1|0}^{C}|\phi\rangle|101\rangle + A_1\Pi_{1|0}^{A}B_1\Pi_{1|0}^{B}\Pi_{0|0}^{C}|\phi\rangle|110\rangle \\
&+ A_1\Pi_{1|0}^{A}B_1\Pi_{1|0}^{B}C_1\Pi_{1|0}^{C}|\phi\rangle|111\rangle\| \\
\leq&\|\Pi_{0|0}^{A}\Pi_{0|0}^{B}\Pi_{0|0}^{C}|\phi\rangle|000\rangle\| + \|\Pi_{0|0}^{A}B_1\Pi_{1|0}^{B}C_1\Pi_{1|0}^{C}|\phi\rangle|011\rangle\| + \\
&\|A_1\Pi_{1|0}^{A}\Pi_{0|0}^{B}C_1\Pi_{1|0}^{C}|\phi\rangle|101\rangle\| + \|A_1\Pi_{1|0}^{A}B_1\Pi_{1|0}^{B}\Pi_{0|0}^{C}|\phi\rangle|110\rangle\| \\
&+ \|A_1\Pi_{1|0}^{A}B_1\Pi_{1|0}^{B}C_1\Pi_{1|0}^{C}|\phi\rangle|111\rangle\| \\
=&|\langle\phi|\Pi_{0|0}^{A}\Pi_{0|0}^{B}\Pi_{0|0}^{C}|\phi\rangle| + |\langle\phi|\Pi_{0|0}^{A}\Pi_{1|0}^{B}\Pi_{1|0}^{C}|\phi\rangle| \\
&+ |\langle\phi|\Pi_{1|0}^{A}\Pi_{0|0}^{B}\Pi_{1|0}^{C}|\phi\rangle| + |\langle\phi|\Pi_{1|0}^{A}\Pi_{1|0}^{B}\Pi_{0|0}^{C}|\phi\rangle| \\
&+ |\langle\phi|\Pi_{1|0}^{A}\Pi_{1|0}^{B}\Pi_{1|0}^{C}|\phi\rangle| \\
=&\varepsilon_{16} + \varepsilon_{17} + \varepsilon_{18} + \varepsilon_{19} + \varepsilon_{20} \\
=&\delta_2.
\end{aligned} \tag{A.20}$$

Thus, we then obtain the distance as

$$\|\Psi(|\phi\rangle_{\mathcal{ABC}} \otimes |000\rangle_{\mathcal{A'B'C'}}) - \sqrt{3}\Pi_{0|0}^{A}\Pi_{0|0}^{B}\Pi_{0|0}^{C}|\phi\rangle_{\mathcal{ABC}} \otimes |W_3\rangle_{\mathcal{A'B'C'}}\| \leq 3\delta_1 + \delta_2. \tag{A.21}$$

The norm of $\sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\left|\phi\right\rangle_{\mathcal{ABC}} \otimes \left|W_3\right\rangle_{\mathcal{A'B'C'}}$ can be estimated,

$$\begin{aligned}
&\|\sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\left|\phi\right\rangle_{\mathcal{ABC}} \otimes \left|W_3\right\rangle_{\mathcal{A'B'C'}}\|^2 = \|\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}C_1\left|\phi\right\rangle(\left|001\right\rangle + \left|010\right\rangle + \left|100\right\rangle)\|^2\\
=&3\|\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}C_1\left|\phi\right\rangle\|^2 = 3|\left\langle\phi\right| X_C\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}C_1\left|\phi\right\rangle|\\
=&3|\left\langle\phi\right| X_C\Pi^A_{0|0}\Pi^B_{0|0}(\Pi^C_{0|0}C_1 - C_1\Pi^C_{1|0} + C_1\Pi^C_{1|0})\left|\phi\right\rangle|\\
\leq&3|\left\langle\phi\right| X_C\Pi^A_{0|0}\Pi^B_{0|0}(\Pi^C_{0|0}C_1 - C_1\Pi^C_{1|0})\left|\phi\right\rangle|\\
&+3|\left\langle\phi\right| X_C\Pi^A_{0|0}\Pi^B_{0|0}C_1\Pi^C_{1|0})\left|\phi\right\rangle|\\
\leq&3\|\Pi^B_{0|0}X_C\left|\phi\right\rangle\|\cdot\|\Pi^A_{0|0}(\Pi^C_{0|0}C_1 - C_1\Pi^C_{1|0})\left|\phi\right\rangle\|\\
&+3|\left\langle\phi\right| X_C\Pi^A_{0|0}\Pi^B_{0|0}C_1\Pi^C_{1|0})\left|\phi\right\rangle|\\
\leq&3\cdot\delta_1 + 3|\left\langle\phi\right| X_C^2\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{1|0})\left|\phi\right\rangle|\\
=&1 - 3\varepsilon_1 + 3\delta_1,
\end{aligned} \tag{A.22}$$

and,

$$\begin{aligned}
&\|\sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\left|\phi\right\rangle_{\mathcal{ABC}} \otimes \left|W_3\right\rangle_{\mathcal{A'B'C'}}\|^2\\
=&3|\left\langle\phi\right| X_C\Pi^A_{0|0}\Pi^B_{0|0}(\Pi^C_{0|0}C_1 - C_1\Pi^C_{1|0} + C_1\Pi^C_{1|0})\left|\phi\right\rangle|\\
\geq&3|\left\langle\phi\right| X_C\Pi^A_{0|0}\Pi^B_{0|0}C_1\Pi^C_{1|0})\left|\phi\right\rangle|\\
&-3|\left\langle\phi\right| X_C\Pi^A_{0|0}\Pi^B_{0|0}(\Pi^C_{0|0}C_1 - C_1\Pi^C_{1|0})\left|\phi\right\rangle|\\
\geq&1 - 3\varepsilon_1 - 3\delta_1.
\end{aligned} \tag{A.23}$$

These results imply that,

$$\|\sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\left|\phi\right\rangle_{\mathcal{ABC}} \otimes \left|W_3\right\rangle_{\mathcal{A'B'C'}} - \left|\text{junk}\right\rangle_{ABC}\left|W_3\right\rangle_{A'B'C'}\| \leq 1 - \sqrt{1 - 3\varepsilon_1 - 3\delta_1} \tag{A.24}$$

where,

$$\left|\text{junk}\right\rangle_{ABC}\left|W_3\right\rangle_{A'B'C'} = \frac{\sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\left|\phi\right\rangle_{\mathcal{ABC}} \otimes \left|W_3\right\rangle_{\mathcal{A'B'C'}}}{\|\sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\left|\phi\right\rangle_{\mathcal{ABC}} \otimes \left|W_3\right\rangle_{\mathcal{A'B'C'}}\|}. \tag{A.25}$$

Finally,

$$\begin{aligned}
&\|\Psi(|\phi\rangle_{\mathcal{ABC}}\otimes|000\rangle_{\mathcal{A'B'C'}})-|\text{junk}\rangle_{ABC}\,|W_3\rangle_{A'B'C'}\,\|\\
\leq&\|\Psi(|\phi\rangle_{\mathcal{ABC}}\otimes|000\rangle_{\mathcal{A'B'C'}})-\sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\,|\phi\rangle_{\mathcal{ABC}}\otimes|W_3\rangle_{\mathcal{A'B'C'}}\,\|\\
&+\|\sqrt{3}\Pi^A_{0|0}\Pi^B_{0|0}\Pi^C_{0|0}\,|\phi\rangle_{\mathcal{ABC}}\otimes|W_3\rangle_{\mathcal{A'B'C'}}-|\text{junk}\rangle_{ABC}\,|W_3\rangle_{A'B'C'}\,\|\\
=&3\delta_1+\delta_2+1-\sqrt{1-3\varepsilon_1-3\delta_1}. \qquad \text{(A.26)}
\end{aligned}$$

As we have said, without losing the generality, we take the maximum ε among ε_is for notational simplicity. Then the relaxed observation requirement will not affect the robustness bound proved below. So a conservative upper bound will be

$$\begin{aligned}
\|\Psi(|\phi\rangle_{\mathcal{ABC}}\otimes|000\rangle_{\mathcal{A'B'C'}})-|\text{junk}\rangle_{ABC}\,|W_3\rangle_{A'B'C'}\,\|&\\
&\leq\frac{13}{2}\varepsilon+9(2+2\sqrt{2})(\frac{20}{3})^{\frac{1}{4}}\frac{9\sqrt{15}+6\sqrt{5}}{20}\varepsilon^{\frac{3}{4}}\\
&+9(2+2\sqrt{2})(\frac{20}{3})^{\frac{1}{4}}\varepsilon^{\frac{1}{4}}\\
&\approx 7.5\varepsilon+119.2\varepsilon^{\frac{3}{4}}+49.4\varepsilon^{\frac{1}{4}}. \qquad \text{(A.27)}
\end{aligned}$$

Thus, the fidelity could be estimated as

$$\begin{aligned}
F=1-&\frac{\|\Psi(|\phi\rangle_{\mathcal{ABC}}\otimes|000\rangle_{\mathcal{A'B'C'}})-|\text{junk}\rangle_{ABC}\,|W_3\rangle_{A'B'C'}\,\|^2}{2} \qquad \text{(A.28)}\\
\approx& 1-12.35\varepsilon^{\frac{1}{2}}-2944.2\varepsilon-185.25\varepsilon^{\frac{5}{4}}. \qquad \text{(A.29)}
\end{aligned}$$

Bibliography

[1] 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.

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

[3] John S. Bell. On the Einstein Podolsky Rosen Paradox. *Physics*, **1**, 195–200, 1964.

[4] A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.*, **47**, 777–780, 1935.

[5] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, **24**, 3, 379–385, 1994.

[6] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2011.

[7] Arthur Fine. Hidden Variables, Joint Probability, and the Bell Inequalities. *Phys. Rev. Lett.*, **48**, 291–295, 1982.

[8] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, **86**, 419–478, 2014.

[9] Valerio Scarani. The device-independent outlook on quantum physics. *Acta Phys. Slov.*, **62**, 4, 347–409, 2012.

[10] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the Set of Quantum Correlations. *Phys. Rev. Lett.*, **98**, 010401, 2007.

[11] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, **10**, 7, 073013, 2008.

[12] M. Froissart. Constructive generalization of Bell's inequalities. *Il Nuovo Cimento B (1971-1996)*, **64**, 2, 241–251, 1981.

[13] Stefano Pironio. Ph.D. thesis, 2004.

[14] Dagomir Kaszlikowski, Leong Chuan Kwek, Jing-Ling Chen, Marek Żukowski, and Choo Hiap Oh. Clauser-Horne inequality for three-state systems. *Physical Review A*, **65**, 3, 032118, 2002.

[15] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. Bell Inequalities for Arbitrarily High-Dimensional Systems. *Phys. Rev. Lett.*, **88**, 040404, 2002.

[16] Jonathan Barrett, Adrian Kent, and Stefano Pironio. Maximally Nonlocal and Monogamous Quantum Correlations. *Phys. Rev. Lett.*, **97**, 170409, 2006.

[17] Reinhard F Werner and Michael M Wolf. Bell inequalities and entanglement. *Quantum Information & Computation*, **1**, 3, 1–25, 2001.

[18] Nicolas Brunner, James Sharam, and Tamás Vértesi. Testing the Structure of Multipartite Entanglement with Bell Inequalities. *Phys. Rev. Lett.*, **108**, 110501, 2012.

[19] Jean-Daniel Bancal, Nicolas Gisin, Yeong-Cherng Liang, and Stefano Pironio. Device-Independent Witnesses of Genuine Multipartite Entanglement. *Phys. Rev. Lett.*, **106**, 250404, 2011.

[20] Stuart J. Freedman and John F. Clauser. Experimental Test of Local Hidden-Variable Theories. *Phys. Rev. Lett.*, **28**, 938–941, 1972.

[21] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental Tests of Realistic Local Theories via Bell's Theorem. *Phys. Rev. Lett.*, **47**, 460–463, 1981.

[22] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedanken experiment* : A New Violation of Bell's Inequalities. *Phys. Rev. Lett.*, **49**, 91–94, 1982.

[23] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin. Experimental demonstration of quantum correlations over more than 10 km. *Phys. Rev. A*, **57**, 3229–3232, 1998.

[24] Bas Hensen, H Bernien, AE Dréau, A Reiserer, N Kalb, MS Blok, J Ruitenberg, RFL Vermeulen, RN Schouten, C Abellán, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, **526**, 7575, 682–686, 2015.

[25] Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. Significant-loophole-free test of Bells theorem with entangled photons. *Phys. Rev. Lett.*, **115**, 25, 250401, 2015.

[26] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam. Strong Loophole-Free Test of Local Realism*. *Phys. Rev. Lett.*, **115**, 250402, 2015.

[27] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzimitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by Bells theorem. *Nature*, **464**, 7291, 1021–1024, 2010.

[28] Le Phuc Thinh, Gonzalo de la Torre, Jean-Daniel Bancal, Stefano Pironio, and Valerio Scarani. Randomness in post-selected events. *New Journal of Physics*, **18**, 3, 035007, 2016.

[29] Thomas Christof, Andreas Lbel, and Sebastian Schenker. PORTA. 1997.

[30] Marcin Pawłowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Żukowski. Information causality as a physical principle. *Nature*, **461**, 7267, 1101–1104, 2009.

[31] Tzyh Haur Yang, Tamás Vértesi, Jean-Daniel Bancal, Valerio Scarani, and Miguel Navascués. Robust and Versatile Black-Box Certification of Quantum Devices. *Phys. Rev. Lett.*, **113**, 040401, 2014.

[32] Jean-Daniel Bancal, Miguel Navascués, Valerio Scarani, Tamás Vértesi, and Tzyh Haur Yang. Physical characterization of quantum devices from nonlocal correlations. *Phys. Rev. A*, **91**, 022115, 2015.

[33] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. In *Computational Complexity, 2009. CCC'09. 24th Annual IEEE Conference on*, pages 217–228. IEEE, 2009.

[34] Tobias Fritz, Tim Netzer, and Andreas Thom. Can you compute the operator norm? *Proceedings of the American Mathematical Society*, **142**, 12, 4265–4276, 2014.

[35] Charles Bennett and Brassard Gilles. Quantum cryptography : Public key distribution and coin tossing. *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, 1984.

[36] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, **67**, 661–663, 1991.

[37] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, **81**, 1301–1350, 2009.

[38] 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.

[39] Stefano Pironio, Antonio Acn, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, **11**, 4, 045021, 2009.

[40] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications*, **2**, 238, 2011.

[41] Sheng-Kai Liao, Hai-Lin Yong, Chang Liu, Guo-Liang Shentu, Dong-Dong Li, Jin Lin, Hui Dai, Shuang-Qiang Zhao, Bo Li, Jian-Yu Guan, et al. Ground test of satellite constellation based quantum communication. *arXiv preprint arXiv:1611.09982*, 2016.

[42] M. W. Johnson, M. H. S. Amin, S. Gildert, T. Lanting, F. Hamze, N. Dickson, R. Harris, A. J. Berkley, J. Johansson, P. Bunyk, E. M. Chapple, C. Enderud, J. P. Hilton, K. Karimi, E. Ladizinsky, N. Ladizinsky, T. Oh, I. Perminov, C. Rich, M. C. Thom, E. Tolkacheva, C. J. S. Truncik, S. Uchaikin, J. Wang, B. Wilson, and G. Rose. Quantum annealing with manufactured spins. *Nature*, **473**, 7346, 194–198, 2011. 10.1038/nature10012.

[43] 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.

[44] Marco Tomamichel and Esther Hnggi. The link between entropic uncertainty and nonlocality. *Journal of Physics A: Mathematical and Theoretical*, **46**, 5, 055301, 2013.

[45] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, **496**, 7446, 456–460, 2013.

[46] Matthew McKague. Interactive proofs for BQP via self-tested graph states. *arXiv preprint arXiv:1309.5675*, 2013.

[47] Matthew Coudron and Henry Yuen. Infinite Randomness Expansion with a Constant Number of Devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 427–436. ACM, New York, NY, USA, 2014.

[48] Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu. Physical randomness extractors: generating random numbers with minimal assumptions. *arXiv preprint arXiv:1402.4797*, 2014.

[49] Sandu Popescu and Daniel Rohrlich. Which states violate Bell's inequality maximally? *Physics Letters A*, **169**, 6, 411 – 414, 1992.

[50] Stephen J. Summers and Reinhard Werner. Maximal violation of Bell's inequalities is generic in quantum field theory. *Communications in Mathematical Physics*, **110**, 2, 247–259, 1987.

[51] Dominic Mayers and Andrew Yao. Self Testing Quantum Apparatus. *Quantum Info. Comput.*, **4**, 4, 273–286, 2004.

[52] 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.

[53] Matthew McKague. Self-testing graph states. *arXiv preprint arXiv:1010.1989*, 2010.

[54] Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A*, **87**, 050102, 2013.

[55] Xingyao Wu, Yu Cai, Tzyh Haur Yang, Huy Nguyen Le, Jean-Daniel Bancal, and Valerio Scarani. Robust self-testing of the three-qubit W state. *Phys. Rev. A*, **90**, 042339, 2014.

[56] Károly F. Pál, Tamás Vértesi, and Miguel Navascués. Device-independent tomography of multipartite quantum states. *Phys. Rev. A*, **90**, 042340, 2014.

[57] Yukun Wang, Xingyao Wu, and Valerio Scarani. All the self-testings of the singlet for two binary measurements. *New Journal of Physics*, **18**, 2, 025021, 2016.

[58] Jedrzej Kaniewski. Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities. *Phys. Rev. Lett.*, **117**, 070402, 2016.

[59] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*, pages 503–509. 1998.

[60] Hajdušek Michal, Pérez-Delgado Carlos A., and Fitzsimons Joseph F. Device-independent verifiable blind quantum computation. *arXiv preprint arXiv:1502.02563*, 2015.

[61] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. *Phys. Rev. A*, **69**, 022308, 2004.

[62] Jens Eisert, Philipp Hyllus, Otfried Gühne, and Marcos Curty. Complete hierarchies of efficient approximations to problems in entanglement theory. *Phys. Rev. A*, **70**, 062317, 2004.

[63] Yonina C Eldar. A semidefinite programming approach to optimal unambiguous discrimination of quantum states. *IEEE Transactions on information theory*, **49**, 2, 446–456, 2003.

[64] O Nieto-Silleras, S Pironio, and J Silman. Using complete measurement statistics for optimal device-independent randomness evaluation. *New Journal of Physics*, **16**, 1, 013035, 2014.

[65] Takesaki Masamichi. *Theory of Operator Algebras I.* Springer, Berlin, 1979.

[66] Adam Bennet, Tamás Vértesi, Dylan J. Saunders, Nicolas Brunner, and G. J. Pryde. Experimental Semi-Device-Independent Certification of Entangled Measurements. *Phys. Rev. Lett.*, **113**, 080405, 2014.

[67] Zhi Zhao, Tao Yang, Yu-Ao Chen, An-Ning Zhang, and Jian-Wei Pan. Experimental Realization of Entanglement Concentration and a Quantum Repeater. *Phys. Rev. Lett.*, **90**, 207901, 2003.

[68] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, Kae Nemoto, W. J. Munro, and Y. Yamamoto. Hybrid Quantum Repeater Using Bright Coherent Light. *Phys. Rev. Lett.*, **96**, 240501, 2006.

[69] Lawrence J. Landau. Empirical two-point correlation functions. *Foundations of Physics*, **18**, 4, 449–460, 1988.

[70] Ll. Masanes. Necessary and sufficient condition for quantum-generated correlations. *arXiv preprint quant-ph/0309137*, 2003.

[71] Ll. Masanes. Extremal quantum correlations for N parties with two dichotomic observables per site. *arXiv preprint quant-ph/0512100*, 2005.

[72] Tsirel'son B.S. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *Foundations of Physics*, **36**, 557–570, 1987.

[73] Carl A Miller and Yaoyun Shi. Optimal robust quantum self-testing by binary nonlocal xor games. *arXiv preprint arXiv:1207.1819*, 2012.

[74] Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing. *Phys. Rev. A*, **91**, 052111, 2015.

[75] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus Nonlocality and Entanglement. *Phys. Rev. Lett.*, **108**, 100402, 2012.

[76] Lucien Hardy. Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories. *Phys. Rev. Lett.*, **68**, 2981–2984, 1992.

[77] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight. Multiparticle entanglement purification protocols. *Phys. Rev. A*, **57**, R4075–R4078, 1998.

[78] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, **53**, 2046–2052, 1996.

[79] Takao Aoki, Go Takahashi, Tadashi Kajiya, Jun-ichi Yoshikawa, Samuel L. Braunstein, Peter van Loock, and Akira Furusawa. Quantum error correction beyond qubits. *Nat. Phys.*, **5**, 541–546, 2009.

[80] J Chiaverini, D Leibfried, T Schaetz, MD Barrett, RB Blakestad, J Britton, WM Itano, JD Jost, E Knill, C Langer, et al. Realization of quantum error correction. *Nature*, **432**, 7017, 602–605, 2004.

[81] Tim Hugo Taminiau, Julia Cramer, Toeno van der Sar, Viatcheslav V Dobrovitski, and Ronald Hanson. Universal control and error correction in multi-qubit spin registers in diamond. *Nature nanotechnology*, **9**, 3, 171–176, 2014.

[82] Robert Raussendorf and Hans J. Briegel. A One-Way Quantum Computer. *Phys. Rev. Lett.*, **86**, 5188–5191, 2001.

[83] Hans J Briegel, David E Browne, W Dür, Robert Raussendorf, and Maarten Van den Nest. Measurement-based quantum computation. *Nature Physics*, **5**, 1, 19–26, 2009.

[84] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Phys. Rev. A*, **69**, 062311, 2004.

[85] Otfried Gühne, Géza Tóth, Philipp Hyllus, and Hans J. Briegel. Bell Inequalities for Graph States. *Phys. Rev. Lett.*, **95**, 120405, 2005.

[86] Pankaj Agrawal and Arun Pati. Perfect teleportation and superdense coding with W states. *Phys. Rev. A*, **74**, 062320, 2006.

[87] Shi-Biao Zheng. Splitting quantum information via W states. *Phys. Rev. A*, **74**, 054303, 2006.

[88] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach. Generalized Schmidt Decomposition and Classification of Three-Quantum-Bit States. *Phys. Rev. Lett.*, **85**, 1560–1563, 2000.

[89] R. F. Werner and M. M. Wolf. All-multipartite Bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, **64**, 032112, 2001.

[90] Marek Żukowski and Časlav Brukner. Bell's Theorem for General N -Qubit States. *Phys. Rev. Lett.*, **88**, 210401, 2002.

[91] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, **65**, 1838–1840, 1990.

[92] M. Ardehali. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. *Phys. Rev. A*, **46**, 5375–5378, 1992.

[93] Belinskiĭ. Interference of light and Bell's theorem.

[94] Ben W Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. *arXiv preprint arXiv:1209.0448*, 2012.

[95] Jonathan Barrett, Daniel Collins, Lucien Hardy, Adrian Kent, and Sandu Popescu. Quantum nonlocality, Bell inequalities, and the memory loophole. *Phys. Rev. A*, **66**, 042111, 2002.

[96] Julia Kempe and Thomas Vidick. Parallel Repetition of Entangled Games. In *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, STOC '11, pages 353–362. ACM, New York, NY, USA, 2011.

[97] André Chailloux and Giannicola Scarpa. Parallel repetition of free entangled games: Simplification and improvements. *arXiv preprint arXiv:1410.4397*, 2014.

[98] R. Jain, A. Pereszlnyi, and P. Yao. A Parallel Repetition Theorem for Entangled Two-Player One-Round Games under Product Distributions. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 209–216. 2014.

[99] I. Dinur, D. Steurer, and T. Vidick. A Parallel Repetition Theorem for Entangled Projection Games. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 197–208. 2014.

[100] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. Detection-Loophole-Free Test of Quantum Nonlocality, and Applications. *Phys. Rev. Lett.*, **111**, 130406, 2013.

[101] Donald H. Pelletier. Merlin's Magic Square. *Am. Math. Monthly*, **94**, 2, 143–150, 1987.

[102] Daniel L. Stock. Merlin's Magic Square Revisited. *The American Mathematical Monthly*, **96**, 7, 608–610, 1989.

[103] P. K. Aravind. Quantum mysteries revisited again. *American Journal of Physics*, **72**, 10, 2004.

[104] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Phys. Rev. A*, **93**, 062121, 2016.

[105] Matthew McKague. Self-testing in parallel with CHSH. *arXiv preprint arXiv:1609.09584*, 2016.

[106] Matthew McKague. Self-testing high dimensional states using the generalized magic square game. *arXiv preprint arXiv:1605.09435*, 2016.

[107] Matthew McKague. Self-testing in parallel. *New Journal of Physics*, **18**, 4, 045013, 2016.

[108] Matthew Coudron and Anand Natarajan. The Parallel-Repeated Magic Square Game is Rigid. *arXiv preprint arXiv:1609.06306*, 2016.

[109] Andrea W Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH. *arXiv preprint arXiv:1609.03687*, 2016.

[110] Anand Natarajan and Thomas Vidick. Robust self-testing of many-qubit states. *arXiv preprint arXiv:1610.03574*, 2016.

[111] Uffe Haagerup and Magdalena Musat. Factorization and Dilation Problems for Completely Positive Maps on von Neumann Algebras. *Communications in Mathematical Physics*, **303**, 2, 555–594, 2011.

[112] Nengkun Yu, Runyao Duan, and Quanhua Xu. Bounds on the distance between a unital quantum channel and the convex hull of unitary channels, with applications to the asymptotic quantum Birkhoff conjecture. *arXiv preprint arXiv:1201.1172*, 2012.