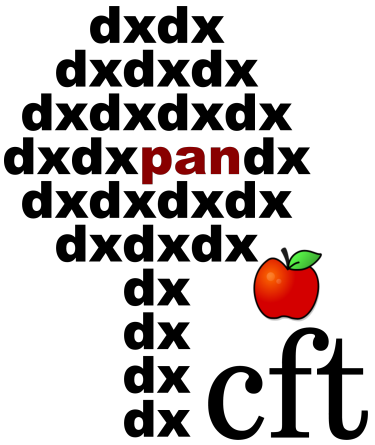
Certification of entangled quantum states and quantum measurements in Hilbert spaces of arbitrary dimension



Author: Shubhayan Sarkar

Supervisor: Dr. Remigiusz Augusiak

Centrum Fizyki Teoretycznej Polskiej Akademii Nauk

A thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Physics

September 2022

Dedicated to my parents, my mother Swapna Sarkar and father Soumen Sarkar,
for making me who I am today.

Abstract

The emergence of quantum theory at the beginning of $20-th$ century has changed our view of the microscopic world and has led to applications such as quantum teleportation, quantum random number generation and quantum computation to name a few, that could never have been realised using classical systems. One such application that has attracted considerable attention lately is device-independent (DI) certification of composite quantum systems. The basic idea behind it is to treat a given device as a black box that given some input generates an output, and then to verify whether it works as expected by only studying the statistics generated by this device. The novelty of these certification schemes lies in the fact that one can almost completely characterise the device (up to certain equivalences) under minimal physically well-motivated assumptions such as that the device is described using quantum theory. The resource required in most of these certification schemes is quantum non-locality.

A lot of work has recently been put into finding DI certification schemes for composite quantum systems. Most of them are however restricted to lower-dimensional systems, in particular two-qubit states. In this thesis, we consider the problem of designing general DI schemes that apply to composite quantum systems of arbitrary local dimensions. First, we construct a fully DI certification scheme, also known as self-testing, that allows us to certify generalised Greenberger-Horne-Zeilinger (GHZ) states of arbitrary local dimension shared among any number of parties from the maximal violation of a certain family of Bell inequalities, for two parties, the generalised GHZ state represents the two-qudit maximally entangled state. Importantly, this is the first instance where such states can be certified using only two measurements per party which is in fact the minimal number of measurements required to observe quantum non-locality.

While a substantial progress has been recently made in designing device-independent certification schemes, most of these schemes are concerned with entangled quantum states. At the same time the problem of certification of quantum measurements remains largely unexplored. In particular, a general scheme allowing one to certify any set of incompatible quantum measurements has not been proposed so far. As designing such a scheme within the DI setting is certainly a difficult task, here we consider a relaxation of the Bell scenario known as the one-sided device-independent (1SDI) scenario. In this scenario, we have an additional assumption that one of the parties is trusted and the measurements performed by this party are known. We propose a scheme for certification of a general class of projective measurements, termed here "genuinely incompatible". To this end, we construct a family of steering inequalities that are maximally violated by any set of genuinely incompatible measurements. Interestingly, mutually unbiased bases belong to this class of measurements. Finally, in the 1SDI scenario, we construct a family of steering

inequalities, whose maximal violation can be used to certify any pure entangled bipartite state using the minimal number of two measurements per observer. Building on this result, we then provide a method to certify any rank-one extremal measurement, including non-projective measurements on the untrusted side.

Interestingly, self-testing of entangled states and measurements can be harnessed to propose schemes to certify that the outcomes of measurements performed on quantum states are perfectly random in the sense that they can not be predicted by an external party. This makes our scheme suitable for quantum cryptographic tasks. We first show that one can generate randomness in a fully DI way using projective measurements from composite quantum states of arbitrary local dimension. Later in the 1SDI scenario, we construct a scheme to certify the optimal amount of randomness that can be generated using a quantum system of any dimension and non-projective extremal measurements, which is twice the amount one can generate using projective measurements.

Streszczenie

Powstanie teorii kwantów na początku XX wieku zmieniło nasz pogląd na świat mikroskopowy i doprowadziło do powstania takich zastosowań efektów kwantowych jak teleportacja kwantowa, kwantowe generowanie liczb losowych i obliczenia kwantowe. Żadne z nich nie mogło by zostać zrealizowane w ramach fizyki klasycznej. Jednym z takich zastosowań, które przyciągnęło ostatnio wiele uwagi, jest certyfikacja złożonych układów kwantowych w wersji niezależnej od urządzeń (ang. *device-independent*). Podstawową jej ideą jest traktowanie danego urządzenia jak czarną skrzynkę, która po podaniu danych wejściowych generuje dane wyjściowe, a następnie wykorzystane obserwowanych statystyk do sprawdzenia, czy urządzenie to działa zgodnie z oczekiwaniami. Nowatorskość schematów certyfikacji tego typu polega na tym, że można prawie całkowicie scharakteryzować urządzenie (z dokładnością do pewnych równoważności) przy minimalnych, dobrze umotywowanych fizycznie założeniach, takich jak to, że urządzenie działa zgodnie z zasadami fizyki kwantowej. Zasobem kwantowym wykorzystywanym przez większość tych schematów certyfikacji jest nielokalność Bella.

Wiele pracy włożono ostatnio w stworzenie schematów certyfikacji w wersji niezależnej od urządzeń dla złożonych układów kwantowych. Większość z nich stosuje się jednak do układów o relatywnie niskich wymiarach lokalnych, w szczególności do stanów dwukubitowych. W tej pracy rozważamy problem projektowania ogólnych schematów, które mają zastosowanie do układów kwantowych o dowolnych wymiarach lokalnych. Najpierw konstruujemy w schemat certyfikacji, znany również jako samotestowanie, który pozwala certyfikować uogólnione stany Greenbergera-Horne'a-Zeilingera (GHZ) o dowolnym wymiarze lokalnym dzielony przez dowolną liczbę obserwatorów na podstawie maksymalnego łamania pewnej rodziny nierówności Bella; w szczególnym przypadku dwóch podukładów stan GHZ sprowadza się do stanu maksymalnie splątanego dwóch kuditów. Co ważne, jest to pierwszy przypadek, w którym takie stany kwantowe mogą być certyfikowane przy użyciu tylko dwóch pomiarów przez każdego z obserwatorów, co jest w rzeczywistości minimalną liczbą pomiarów wymaganą do zaobserwowania nielokalności Bella.

Choć w ostatnich latach dokonano znacznego postępu w projektowaniu schematów certyfikacji w wersji niezależnej od urządzeń, większość z nich dotyczy splątanych stanów kwantowych. Jednocześnie problem certyfikacji pomiarów kwantowych pozostaje w dużej mierze niezbadany. Brakuje w szczególności ogólnego schematu pozwalającego na certyfikację dowolnego zestawu niekompatybilnych pomiarów kwantowych. Ponieważ stworzenie takiego schematu w scenariuszu niezależnym od urządzeń jest trudnym zadaniem, w rozprawie rozważamy pewien uproszczony scenariusz, znany jako scenariusz jednostronnie niezależny od urządzeń (1SDI). W tym scenariuszu czynimy dodatkowe założenie, że

jedno z urządzeń pomiarowych jest w pełni scharakteryzowane i wykonuje znane pomiary kwantowe. Proponujemy schemat certyfikacji ogólnej klasy pomiarów rzutowych, określanych tu jako prawdziwie niekompatybilne. W tym celu konstruujemy rodzinę nierówności sterowania (ang. *steering inequalities*), których maksymalna wartość kwantowa osiągana jest przez dowolny zbiór prawdziwie niekompatybilnych pomiarów. Co ciekawe, do tej klasy pomiarów kwantowych zaliczają się te, które odpowiadają bazom wzajemnie niejednoznacznym. Wreszcie, w scenariuszu 1SDI, konstruujemy rodzinę nierówności sterowania, których maksymalne łamanie może być wykorzystane do certyfikacji dowolnego czystego, splątanego stanu dwucząstkowego przy użyciu minimalnej liczby dwóch pomiarów wykonywanych przez obu obserwatorów. Opierając się na tym wyniku, podajemy następnie metodę certyfikacji dowolnego ekstremalnego pomiaru kwantowego rzędu jeden, włączając w to pomiary nierzutowe.

Co ciekawe, metody samotestowania stanów oraz pomiarów kwantowych mogą być wykorzystane do stworzenia schematów poświadczania, że wyniki pomiarów wykonywanych na stanach kwantowych są losowe w tym sensie, że nie mogą być przewidziane przez żadnego zewnętrznego obserwatora. To sprawia, że nasze wyniki stają się użyteczne w zadaniach kryptograficznych. Najpierw pokazujemy, że ze splątanych stanów kwantowych o dowolnym wymiarze lokalnym można generować losowość w scenariuszu niezależnym od urządzeń używając pomiarów rzutowych. Następnie, w scenariuszu 1SDI, konstruujemy schemat poświadczający optymalną ilość losowości, która może być wygenerowana przy użyciu układu kwantowego o dowolnym wymiarze i nierzutowych pomiarów ekstremalnych, która równa jest dwukrotności maksymalnej ilości losowości, którą można wygenerować przy użyciu pomiarów rzutowych.

Declaration

The work described in this thesis was undertaken between October 2018 and April 2022 while the author was a doctoral student under the supervision of Prof. Remigiusz Augusiak at the Center for Theoretical Physics, Polish Academy of Sciences. All the required coursework was completed between October 2018 and July 2020 at the Institute of Physics, Polish Academy of Sciences. No part of this thesis has been submitted for any other degree at the Center for Theoretical Physics, Polish Academy of Sciences or any other scientific institution.

This thesis is based upon four different research works carried on during the doctoral studies all of which are listed below.

1. **Shubhayan Sarkar**, Remigiusz Augusiak, *Self-testing of multipartite GHZ states of arbitrary local dimension with arbitrary number of measurements per party*, Phys. Rev. A **105**, 032416 (2022).

2. **Shubhayan Sarkar**, Jakub J. Borkała, Chellasamy Jebarathinam, Owidiusz Makuta, Debashis Saha, Remigiusz Augusiak, *Self-testing of any pure entangled state with minimal number of measurements and optimal randomness certification in one-sided device-independent scenario*, arXiv:2110.15176 (2021).

3. **Shubhayan Sarkar**, Debashis Saha, Remigiusz Augusiak, *Certification of incompatible measurements using quantum steering*, arXiv:2107.02937 (2021).

4. **Shubhayan Sarkar**, Debashis Saha, Jędrzej Kaniewski, Remigiusz Augusiak, *Self-testing quantum systems of arbitrary local dimension with minimal number of measurements*, npj Quantum Information **7**, 151 (2021).

In addition to the work presented in this thesis, the author has also carried out the following research tasks all of which are listed below.

1. Jakub Jan Borkała, Chellasamy Jebarathinam, **Shubhayan Sarkar**, Remigiusz Augusiak, *Device-independent certification of maximal randomness from pure entangled two-qutrit states using non-projective measurements*, Entropy **24(3)**, 350 (2022).

2. **Shubhayan Sarkar**, Debashis Saha, *Probing measurement problem of quantum theory with an operational approach*, arXiv:2107.08447 (2021).

3. **Shubhayan Sarkar**, *Universal notion of classicality based on ontological framework*, arXiv:2104.14355 (2021).

4. Colin Benjamin, **Shubhayan Sarkar**, *Emergence of Cooperation in the thermodynamic limit*, Chaos, Solitons & Fractals **135**, 109762 (2020).

5. Colin Benjamin, **Shubhayan Sarkar**, *Triggers for cooperative behavior in the thermodynamic limit: a case study in Public goods game*, Chaos **29**, 053131 (2019).

6. **Shubhayan Sarkar**, Colin Benjamin, *Quantum Nash equilibrium in the thermodynamic limit*, Quantum Inf. Process. **18**, 122 (2019).

7. **Shubhayan Sarkar**, Colin Benjamin, *Entanglement makes free riding redundant in the thermodynamic limit*, Physica A: Statistical Mechanics and its Applications **521**, 607 (2019).

8. **Shubhayan Sarkar**, *Entropy as a bound for expectation values and variances of a general quantum mechanical observable*, International Journal of Quantum Information, **16** 1850036 (2018).

9. **Shubhayan Sarkar**, Chandan Datta, *Can quantum correlations increase in a quantum communication task?*, Quantum Inf Process **17**, 248 (2018).

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor, Remigiusz Augusiak. This thesis would not have been completed without his support and constant encouragement. He always helped me whenever I was stuck in academic as well as administrative problems. At all times, he was understanding and willing to help.

Furthermore, I feel indebted to thank Center for Theoretical Physics of the Polish Academy of Sciences for providing me with the research environment and also to the administrative team, whom I troubled a lot during my studies. Not to mention, they were a constant support and helped me even with my personal difficulties.

This thesis would not have been possible without the help of my group members Debashis Saha, Gautam Sharma, Jakub J. Borkała, Chellasamy Jebarathinam and Owidiusz Makuta and also Jędrzej Kaniewski, who were involved in the research tasks that finally led to this thesis. I would like to thank my friends Chandan Datta, Rubina Ghosh, Kaustav Sengupta, Sudeep Sarkar, Saubhik Sarkar, Suparna Saha, Ishika Palit, Suhani Gupta, Kiran Saba, Saikruba Krishnan, Rafael Santos, Julius Serbenta, Grzegorz Rajchel-Mieldzioc and Michele Grasso.

I would like to thank my family specially my parents who believed in me and were with me in my ups and downs. Also special thanks to Bohnishikha Ghosh for being a constant support.

Finally, I would also like to thank the Foundation for Polish Science for their support through the First Team project (No First TEAM/2017-4/31) co-financed by the European Union under the European Regional Development Fund. The grant not just financed my stay in Poland but also provided opportunities to visit various institutes across Europe to share my research works and learn from the leading experts in the field.

Contents

Chapter 1

Introduction

The advent of quanta by Planck in 1900 for describing black-body radiation marked as the beginning of "quantum era of theoretical physics". With the increasingly precise experiments on microscopic objects, it was soon realised that the structure of atom was not describable with classical physics but required a new non-classical description. In this pursuit, Schrödinger in 1923, using the ideas of Bohr and De-Broglie that microscopic objects might possess both wave and particle characteristics, came up with a wave equation describing the microscopic world, which is now known as the Schrödinger's equation. It is excellently successful in predicting the results of the experiments performed till date. However, the Schrödinger equation involves an object known as a wavefunction, whose meaning was hugely debated and was believed to be just a mathematical object without any physical significance. It was the work of Max Born that established that the wavefunction contains information about the probability of the system being at a particular position in space. This can be considered as one of the biggest paradigm shifts in the human understanding of nature, as the microscopic world might be inherently unpredictable, and the maximum information that can be gained is the probability of the system being at a particular state. Many prominent physicists did not buy this idea and even led Einstein to one of his famous quotes, "God does not play dice". In fact, the unpredictable nature of the microscopic world can be considered as the foundational philosophy behind "quantum theory".

With even more experiments probing the microscopic regime, it was soon realised that quantum theory is the best description of this regime, even when the theory leads to counter-intuitive phenomena and paradoxes. With later works of pioneers like Heisenberg, Bohr, Von-Neumann and Dirac, to name a few, we arrive at four postulates on which quantum theory is based on [cf. [1], [2]].

1. Any state of the system is represented by a density matrix ρ acting on some Hilbert space $\mathscr{H}$.

2. The time evolution of the quantum system is generated by completely positive and trace preserving (CPTP) maps.

3. A system composed of two subsystems A and B is described using a quantum state belonging to the Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$ where $\mathscr{H}_A, \mathscr{H}_B$ are the Hilbert spaces associated with the subsystems A, B respectively.

4. Any measurement to observe the state of the system ρ is represented by a set of positive operators $M = \{E_k\}$ that act on the Hilbert space $\mathscr{H}$. Here k represents the outcome of the measurement and $\sum_k E_k = \mathbb{1}_{\mathscr{H}}$. The probability of observing the the outcome k is denoted by $p(k|M,\rho)$ and can be computed as,

$$p(k|M,\rho) = \mathrm{Tr}(E_k\rho). \tag{1.1}$$

All the notions presented here will later be revisited again in details.

An important step towards the understanding of quantum theory was put forward by Einstein, Podolski and Rosen in 1935 in their seminal paper [3], where it was claimed that quantum theory is incomplete. It was later speculated by physicists like Bohm and Von-Nuemann that an underlying classical-like theory would be able to predict all the quantum effects and would remove all the counter-intuitiveness of the theory. This remained only a theoretical idea until Bell's pioneering work in 1964 [4]. He put forward a way to test whether quantum theory is inherently different from classical physics. It was later confirmed by experiments that any classical description is insufficient to explain some quantum phenomena [5]–[8].

This led to the understanding that there can exist tasks in which strategies involving quantum states and measurements would perform much better than classical strategies, giving birth to the field of quantum information theory. In this thesis, we explore one of the recently contrived areas in quantum information theory, namely device-independent quantum protocols [9] focusing particularly on device-independent certification of quantum states, measurements and intrinsic randomness that can be generated using quantum systems.

The idea of device-independent certification has gained much attention lately, mainly due to their implications in quantum cryptography as well as foundations of quantum theory. Let us say that two spatially separated labs are given a device whose inner mechanism is unknown and thus they can be treated as black boxes. If an input is provided to this device, it produces an output. Based on various inputs and outputs, one can construct the statistics. Assuming that these devices satisfy the rules of quantum theory, any such statistics needs to be explained via quantum measurements acting on some quantum state. The basic idea behind device-independent certification is that using only

the statistics obtained by performing local measurements on a composite quantum system, one can characterise this system and also the measurements up to certain equivalences.

The strongest device-independent certification scheme is known as self-testing where no assumptions on the devices are made apart from the fact that they are governed by quantum theory. The idea of self-testing was first introduced by Mayers and Yao in 1998 [10], [11] in the cryptographic context as a way of certifying that the parties share a desired state. Since then, numerous self-testing schemes for composite quantum systems and measurements have been introduced. For instance Refs. [12]–[21] provide schemes for certification of pure bipartite entangled states that are locally qubits. Then, Refs. [22]–[30] provide methods to certify multipartite states of local dimension two. A few works Refs. [31]–[35] provide certification schemes of entangled states of local dimension higher than two. In [32] (see also [33]) a strategy for certification of every pure bipartite entangled state was introduced.

In Chapter 3 of this thesis, we provide a general scheme that self-tests the generalised Greenberger-Horne-Zeilenger (GHZ) state [36] of arbitrary local dimension shared among arbitrary number of parties. Restricting to two parties, the above state is, in fact, the maximally entangled state of arbitrary local dimension. Unlike the previous self-testing scheme [32] that allows for certification of arbitrary dimensional states, we use the minimum possible number of measurements per party, that is, two. This is particularly useful from an application point of view, as it reduces the experimental effort necessary to implement our scheme. With the aim to self-test measurements, we generalise this scheme to arbitrary number of measurements per party. An important application of our self-testing scheme is towards device-independent certification of genuine randomness. Sources generating genuine randomness are useful in many areas such as numerical computation or cryptography. We provide a scheme for certifying the maximum amount of randomness that can be extracted from a quantum system of arbitrary local dimension using projective measurements. This chapter is based on two of our works, [37] and [38]. The first one proves self-testing statement for the maximally entangled state of two qudits based on the maximal violation of the SATWAP Bell inequality introduced in [39]. The second paper generalises this result to the GHZ state shared among arbitrary number of parties based on the maximal violation of ASTA Bell inequality introduced in [40].

Any quantum device consists mainly of two parts: a source that generates a quantum state and a measuring device that performs a measurement on this state. While there has been considerable progress in designing self-testing schemes for quantum states, the avenue for certification of quantum measurements remains largely unexplored. Recently, in [41] and [42], the authors introduced a way of self-testing the bases of the set of two-outcome and three-outcome observables respectively. Apart from a few results [19], [31], [32], [43]–[48], there is no general method allowing to certify any set of incompatible

measurements.

To simplify the problem, depending on the physical scenario, one can make some assumptions about the quantum devices. In this thesis, we consider a scheme in which one of the parties is trusted, known as one-sided device-independent (1SDI) scenario. The resource that one needs here to certify quantum states or measurements is known as quantum steering, which is another form of quantum non-locality [49], [50]. The quantum steering scenario is similar to the Bell scenario, apart from the fact that one of the parties is trusted, or equivalently, that the measurement device of the trusted party performs known measurements. The first 1SDI certification scheme was introduced in 2016 [51] (see also [52]). Their scheme allows for certification of the two-qudit maximally entangled state and two binary outcome measurements.

In Chapter 4 of this thesis, we provide the first certification scheme that applies to a general family of incompatible projective measurements which we termed "genuinely incompatible". An important class of projective measurements that are well-studied in quantum information theory are those corresponding to mutually unbiased bases. For instance, they are crucial for the security of quantum cryptographic tasks [53]–[57]. Also, there is a close link between mutually unbiased bases and quantum cloning [58]–[60] (see [61], for a review on mutually unbiased bases). As a matter of fact, we show that mutually unbiased bases are also genuinely incompatible, and thus we provide a certification scheme of mutually unbiased bases of arbitrary dimension. For two observables corresponding to mutually unbiased bases, we also find the robustness of our scheme against experimental errors, which makes it relevant for practical applications. This chapter is based on our work [62].

Recently, quantum non-locality has been realised as an effective way to generate genuine randomness and device-independently verify that there is no intruder who has access to it [63]–[65]. The maximum amount of randomness that one can, in principle, obtain from a quantum system of a dimension d is $2\log_2 d$ bits. A long-standing question in quantum information theory is whether one can find protocols that can be used to certify this maximal amount of randomness.

In Chapter 5 of this thesis, we again consider the one-sided device-independent scenario. We begin by devising a 1SDI scheme that can be used to certify any pure bipartite entangled state. Importantly, our scheme utilises only two measurements per party, which is the minimal number of measurements necessary to observe quantum steering. Moreover, these measurements are independent of the state to be certified. This makes our scheme much easier to implement in experiments. Using these results, we provide a scheme for certification of any rank-one extremal generalised measurements. This allows us to finally certify the maximal amount of randomness that one can generate from a quantum system of any dimension. We further show for some dimensions that the amount of randomness is

independent of the amount of entanglement in the quantum system.This chapter is based on our work [66].

Before presenting the main results of this thesis, in Chapter 2 we introduce the relevant technical concepts and notions which will be required throughout this thesis. The thesis ends with concluding remarks and a list of open problems in Chapter 6.

Chapter 2

Technical introduction

2.1 Basics of quantum information theory

Let us begin by elaborating on the four postulates of quantum theory presented in Introduction.

2.1.1 States in quantum theory

Definition 1 (Pure quantum states)**.** *Pure quantum states are normalised vectors belonging to a Hilbert space $\mathscr{H}$ and are denoted by $|\psi\rangle$. The normalisation condition ensures that*

$$\langle\psi|\psi\rangle = 1. \tag{2.1}$$

In general, the state $|\psi\rangle$ can belong to Hilbert space of infinite dimension. However in this work, we consider only finite-dimensional Hilbert spaces. Any pure quantum state $|\psi\rangle \in \mathscr{H}$ such that the dimension of the Hilbert space is d, can be expressed using a set of d linearly independent vectors, $\mathscr{B} = \{|e_i\rangle\}_{i=0}^{d-1}$ known as a basis. Now, any quantum system belonging to a $d-$dimensional Hilbert space is known as qudit. A two dimensional quantum system is known as qubit. An important basis that is widely used in quantum information theory and will be extensively used in this work is known as the computational or standard basis, represented by $\mathscr{B}_c = \{|i\rangle\}_i$, where

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots \quad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}. \tag{2.2}$$

Note that the elements in the basis $\mathscr{B}_c$ are orthogonal, that is, $\langle i|j\rangle = \delta_{i,j}$ where

$$\delta_{i,j} = \begin{cases} 1 & \text{if} \quad i = j \\ 0 & \text{if} \quad i \neq j \end{cases} . \tag{2.3}$$

In certain situations, considered also in this thesis, one needs to use density matrices denoted by ρ to describe a quantum system. These are matrices acting on the Hilbert space $\mathscr{H}$ that satisfy the following properties

$$\text{Tr}(\rho) = 1, \quad \rho \geq 0, \quad \text{and} \quad \rho = \rho^\dagger, \tag{2.4}$$

that is, they are normalised and positive semi-definite. For any pure state $|\psi\rangle$, the corresponding density matrix is given by $\rho_p = |\psi\rangle\langle\psi|$.

Definition 2 (Mixed states)**.** *Quantum states that can be written as convex combination of other quantum states, are known as mixed states, that is,*

$$\rho_m = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{2.5}$$

For a note, a particular decomposition of ρ_m (2.5) is not unique.

Let us now consider the scenario when a system consists of two subsystems A and B. Let $\mathscr{H}_A$ and $\mathscr{H}_B$ denote the Hilbert spaces of A and B respectively. According to the postulates of quantum theory the Hilbert space of their joint system is given by $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$. In such composite systems, we can have two major classes of states, separable and entangled. Let us begin with pure separable states also known as product states.

Definition 3 (Product states)**.** *Consider a pure state $|\psi_{AB}\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$. We call it a product state if it can be written as $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$ where $|\psi\rangle_A \in \mathscr{H}_A$ and $|\psi\rangle_B \in \mathscr{H}_B$.*

Definition 4 (Separable States [67])**.** *A mixed state ρ_{sep} acting on $\mathscr{H}_A \otimes \mathscr{H}_B$ is called separable if it can be written as convex mixture of product states.*

Thus, any separable state can be written as

$$\rho_{sep} = \sum_i p_i |\psi_i\rangle_A\langle\psi_i| \otimes |\phi_i\rangle_B\langle\phi_i| \tag{2.6}$$

where $|\psi_i\rangle_A \in \mathscr{H}_A$ and $|\phi_i\rangle_B \in \mathscr{H}_B$. Let us now look at a class of states that do not exist in classical physics.

Definition 5 (Entangled States)**.** *Quantum states that are not separable as defined in Def. 4 are classified as entangled states.*

For example, when both the Hilbert spaces of A and B is $\mathbb{C}^2$, then the quantum state

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \tag{2.7}$$

is entangled.

A convenient way to express any pure bipartite state, that is quantum systems consisting of only two subsystems, $|\psi\rangle_{AB} \in \mathscr{H}_{AB}$ is by using the Schmidt decomposition [2]. Let us say Hilbert space of subsystem A, denoted by $\mathscr{H}_A$ is of dimension m and Hilbert space of subsystem B, denoted by $\mathscr{H}_B$ is of dimension n, then any state $|\psi\rangle_{AB}$ can be written as

$$|\psi\rangle_{AB} = \sum_{i=1}^{\min\{m,n\}} \lambda_i |e_i\rangle \otimes |f_i\rangle \tag{2.8}$$

such that $\lambda_i \geq 0$ with $\sum_i \lambda_i^2 = 1$ and $\{|e_i\rangle\}$, $\{|f_i\rangle\}$ are set of orthonormal vectors defined on $\mathscr{H}_A$ and $\mathscr{H}_B$ respectively[1].

Let us now consider quantum systems consisting of N subsystems where N is any positive integer greater than two such that the local Hilbert spaces are denoted by $\mathscr{H}_i$ for $i = 1, 2, \ldots, N$. Then such a state is described by a density matrix ρ_N acting on $\mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \ldots \otimes \mathscr{H}_N$. We can straightforwardly generalise the notion of separability and entanglement to the multipartite states as done above. This completes the classification of quantum states. We now move on to characterising dynamics in quantum theory.

2.1.2 Dynamics in quantum theory

Within quantum theory, any evolution in general is represented by completely positive and trace preserving (CPTP) maps. However, in this work we restrict ourselves to a family of maps that are known as unitary transformations or unitary matrices.

Definition 6 (Unitary transformation)**.** *A unitary transformation U is a mapping from a Hilbert space $\mathscr{H}$ to $\mathscr{H}$ that preserves the distance between any two vectors belonging to $\mathscr{H}$.*

A unitary matrix U acting on $\mathscr{H}$ is characterised by the following properties,

$$UU^\dagger = \mathbb{1} \quad \text{or} \quad U^{-1} = U^\dagger, \tag{2.9}$$

that is, the inverse of any unitary matrix is equal to its conjugate transpose. Interestingly, any CPTP map can be realised as a unitary map acting on some higher dimensional system

[1]For ease of mathematical notation, most of the times the symbol "$\otimes$" will be dropped.

[68]. In fact, the dynamics of closed quantum systems are reproduced by unitary maps. Another class of CPTP maps that is relevant for this work is known as isometry [69].

Definition 7 (Isometry)**.** *An isometry is generalisation of a unitary matrix, mapping one Hilbert space $\mathscr{H}$ of lower dimension to some other Hilbert space $\mathscr{H}'$ of higher dimension in a way that preserves the distance between any two vectors belonging the Hilbert space $\mathscr{H}$.*

We now move on to characterising measurements in quantum theory.

2.1.3 Measurements in quantum theory

Any measurement M with m outcomes in quantum theory is defined by the set of positive operators $\{E_k\}$ that act on some Hilbert space $\mathscr{H}$ for $k = 0, 1, 2, \ldots, m-1$. These positive operators are hermitian, that is, $E_k = E_k^\dagger$ and sum up to identity $\sum_k E_k = \mathbb{1}_{\mathscr{H}}$ which is a consequence of the fact that the probabilities of outcomes must sum up to 1. Due to this, measurements in quantum theory are also referred to as positive-operator valued measures or simply POVM's. The probability of observing the outcome k if the measurement M has been performed on a state $\rho \in \mathscr{H}$ is given by,

$$p(k|M,\rho) = \mathrm{Tr}(E_k\rho). \tag{2.10}$$

It is clear to see from the above expression that $\sum_k p(k|M,\rho) = 1$. Let us now try to understand the idea of normalisation of the state as discussed in the previous subsection 2.1. Suppose that state of the quantum system is $|\psi\rangle$. Now, we consider a two-outcome measurement M_2 with measurement elements

$$E_0 = |\psi\rangle\langle\psi|, \quad \text{and} \quad E_1 = \mathbb{1} - |\psi\rangle\langle\psi|. \tag{2.11}$$

Then the probability of observing the system in the quantum state $|\psi\rangle$ must be 1 or equivalently, the measurement must always output the 0^{th} outcome. Thus, we have that

$$p(0|M_2, |\psi\rangle\langle\psi|) = |\langle\psi|\psi\rangle|^2 = 1. \tag{2.12}$$

Consequently, the quantum state must be normalised so that the total probability of finding the system in any quantum state is one.

Quantum measurements for a given Hilbert space form a convex set. Now, we look at a special class of POVM's that lie at the boundary of this set.

Definition 8 (Extremal POVM's)**.** *Any POVM that can not be written as a convex combination of other POVM's is called extremal.*

As was proven in [70], the measurement operators of any rank-one extremal POVM can be written as $E_k = \lambda_k \Pi_k$, where

$$\Pi_k = |\psi_k\rangle\langle\psi_k| \tag{2.13}$$

and $\lambda_k \geq 0$. Moreover, $E_k's$ are linearly independent for all k. It was further proven in [70] that for POVM's that act on a Hilbert space $\mathscr{H}$ of dimension d, an extremal POVM can have atmost d^2 outcomes. Any other POVM can be written as convex combination of extremal POVM's. A special class of extremal POVM's, are known as projective measurements.

Definition 9 (Projective measurements)**.** *Projective measurements are POVM's where the measurement elements are represented by projectors* Π_i *such that* $\Pi_i\Pi_j = \delta_{i,j}\Pi_i$.

For any rank-one projective measurement, the corresponding measurement elements are given by $E_k = \Pi_k = |\psi_k\rangle\langle\psi_k|$. Along with the condition that $\sum_k \Pi_k = \mathbb{1}_{\mathscr{H}}$ and $\Pi_i\Pi_j = \delta_{i,j}\Pi_i$, it can be concluded that $\{|\psi_k\rangle\}$ for all $k's$ form a complete basis of the Hilbert space $\mathscr{H}$ which the measurement acts on. The state of the system after the measurement is performed on it is known as the post-measurement state. For instance, let us consider the measurement $\{E_k\}$ and a quantum state ρ, then the post-measurement state ρ^a_{pm} after the outcome a is observed is given by,

$$\rho^a_{pm} = \frac{\sqrt{E_a}\rho\sqrt{E_a}}{\mathrm{Tr}(E_a\rho)} \qquad \forall a. \tag{2.14}$$

An equivalent way to represent measurements in quantum theory is by using quantum observables. Let us first consider the simplest scenario where the measurements have only two outcomes and are projective. The quantum observable $\mathbb{A}$ corresponding to such a measurement $M = \{\Pi_0, \Pi_1\}$ is represented by,

$$\mathbb{A} = \Pi_0 - \Pi_1. \tag{2.15}$$

From the above expression, we can conclude that such quantum observables are hermitian and unitary,

$$\mathbb{A} = \mathbb{A}^\dagger, \quad \text{and} \quad \mathbb{A}\mathbb{A}^\dagger = \mathbb{1}. \tag{2.16}$$

One can define the expectation value of $\mathbb{A}$ in terms of the probabilities of obtaining outcome $0,1$ as

$$\langle\mathbb{A}\rangle_\rho = \mathrm{Tr}(\mathbb{A}\rho) = p(0|M,\rho) - p(1|M,\rho). \tag{2.17}$$

The above construction of quantum observables can also be generalised to two-outcome POVM's where $\mathbb{A} = E_0 - E_1$. However, such an observable is not unitary. This construction of quantum observables was generalised to arbitrary outcome POVM's in [31]. We refer them here as generalised observables. Consider a $d-$outcome measurement. One defines generalised expectation values $\langle \mathbb{A}^{(l)} \rangle_\rho$ for $l = 0, 1, \ldots, d-1$ as the Fourier transform of the probabilities $p(k|M,\rho)$ as,

$$\langle \mathbb{A}^{(l)} \rangle_\rho = \sum_{k=0}^{d-1} \omega^{lk} p(k|M,\rho) \quad \text{for} \quad l = \{0,1,\ldots,d-1\} \tag{2.18}$$

where $\omega = e^{2\pi i/d}$ is the $d-th$ root of unity. Notice that using inverse Fourier transform, we can obtain the probabilities from the expectation values as,

$$p(k|M,\rho) = \frac{1}{d} \sum_{l=0}^{d-1} \omega^{-lk} \langle \mathbb{A}^{(l)} \rangle_\rho \quad \text{for} \quad k = \{0,1,\ldots,d-1\} \tag{2.19}$$

Using the above definition (2.18), analogous to the two-outcome case, one can define the following expression for the corresponding observables $\mathbb{A}^{(l)}$ in terms of the measurement elements E_k

$$\mathbb{A}^{(l)} = \sum_{k=0}^{d-1} \omega^{lk} E_k \quad \text{for} \quad l = \{0,1,\ldots,d-1\}. \tag{2.20}$$

Equivalently the measurement elements E_k can be obtained from the quantum observables $\mathbb{A}^{(l)}$ by considering the inverse Fourier transform,

$$E_k = \frac{1}{d} \sum_{l=0}^{d-1} \omega^{-lk} \mathbb{A}^{(l)} \quad \text{for} \quad k = \{0,1,\ldots,d-1\}. \tag{2.21}$$

Some relevant properties about the observable $\mathbb{A}^{(l)}$ can be obtained from Eq. (2.20) such as,

$$\mathbb{A}^{(d)} = \mathbb{1}, \quad \text{and} \quad \mathbb{A}^{(d-l)} = \mathbb{A}^{(-l)} = \mathbb{A}^{(l)\dagger} \tag{2.22}$$

along with

$$\mathbb{A}^{(l)} \mathbb{A}^{(l)\dagger} \leq \mathbb{1}, \qquad \text{and} \qquad \mathbb{A}^{(l)\dagger} \mathbb{A}^{(l)} \leq \mathbb{1}, \tag{2.23}$$

where to obtain the relations (2.22) we used the fact that $\sum_k E_k = \mathbb{1}$ and $E_k = E_k^\dagger$. The relation (2.23) was proven in [31]. An important result about generalised observables that are unitary was also proven in [31].

Fact 1. *Consider the generalised observables* $\mathbb{A}^{(l)}$ *as defined in* (2.20)*. These observables are unitary, that is,*

$$\mathbb{A}^{(l)}\mathbb{A}^{(l)\dagger} = \mathbb{1}, \quad \textit{and} \quad \mathbb{A}^{(l)} = \mathbb{A}^{l} \quad \forall l \tag{2.24}$$

if and only if the corresponding measurement is projective, that is, $E_k E_{k'} = \delta_{k,k'} E_k$ *for every* k, k'*.*

This fact will be used extensively throughout this thesis. Often at times, the generalised observables $\mathbb{A}^{(l)}$ would be referred to as measurements as they contain all the information to reconstruct the actual measurement. Consider now a multipartite system and on each subsystem a local measurement $M_i = \{E_{i,k}\}$ is performed where $i = 1, 2, \ldots, N$ denotes the subsystems. The probability to obtain outcomes $k_1, k_2, \ldots k_N$ when the measurements are performed on a state ρ_N acting on $\mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \ldots \otimes \mathscr{H}_N$,

$$p(k_1, k_2, \ldots, k_N | \rho_N) = \mathrm{Tr}(E_{1,k_1} \otimes E_{2,k_2} \otimes \ldots E_{N,k_N} \rho_N) \tag{2.25}$$

The notion for the observables can also be generalised to the multipartite case

$$\mathbb{A}_1^{(l_1)} \otimes \mathbb{A}_2^{(l_2)} \otimes \ldots \otimes \mathbb{A}_N^{(l_N)} = \sum_{k_1, k_2, \ldots, k_N = 0}^{d-1} \omega^{l_1 k_1 + l_2 k_2 + \ldots l_N k_N} E_{1,k_1} \otimes E_{2,k_2} \otimes \ldots \otimes E_{N,k_N}. \tag{2.26}$$

for every $l_1, l_2, \ldots, l_N$.

An important distinction between any classical and quantum theories is the existence of quantum measurements that are mutually incompatible. Two projective measurements M_1 and M_2 are mutually incompatible, if these two measurements do not commute. For example, consider the Pauli observables σ_z and σ_x corresponding to projective measurements that acts on qubits in z and x direction respectively

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{and} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.27}$$

are incompatible. For a review of incompatibility of quantum measurements refer to [71], [72].

2.1.4 Purification of quantum states and measurements

Another important concept for multipartite quantum systems is the extraction of the local quantum state for each subsystem given some global quantum state. For simplicity, we review it here for bipartite quantum systems but the concept can be straightforwardly

generalised to the multipartite case. Let us suppose the global quantum state is given by ρ_{AB}, then the local quantum states ρ_A and ρ_B are given by

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) \quad \text{and} \quad \rho_B = \mathrm{Tr}_A(\rho_{AB}) \tag{2.28}$$

where Tr_B and Tr_A denote partial trace over the subsystem B and A respectively and are computed as,

$$\mathrm{Tr}_x(\rho_{AB}) = \sum_j \langle j_x|\rho_{AB}|j_x\rangle \qquad (x = A,B), \tag{2.29}$$

where $\{|j_x\rangle\}$ is any orthonormal basis than spans the Hilbert space $\mathscr{H}_x$ of the subsystem x with $x = A,B$. For any separable state ρ_{sep} [cf. Def. 4] using Eq. (2.6), the local quantum states of the subsystem A can be simply computed as

$$\rho_A = \mathrm{Tr}_B(\rho_{sep}) = \sum_i p_i |\psi_i\rangle_A\langle\psi_i| \otimes \mathrm{Tr}\left(|\phi_i\rangle_B\langle\phi_i|\right). \tag{2.30}$$

Using the fact that $\mathrm{Tr}\left(|\phi_i\rangle_B\langle\phi_i|\right) = 1$, we arrive at

$$\rho_A = \mathrm{Tr}_B(\rho_{sep}) = \sum_i p_i |\psi_i\rangle_A\langle\psi_i|. \tag{2.31}$$

Analogously, the local quantum state of the subsystem B is given by,

$$\rho_B = \mathrm{Tr}_A(\rho_{sep}) = \sum_i p_i |\phi_i\rangle_B\langle\phi_i|. \tag{2.32}$$

Computing the local quantum states of subsystem A and B when they are entangled is not as straightforward as separable states. For an example, let us consider a pure bipartite entangled state of local dimension d given by,

$$|\psi\rangle_{AB} = \sum_{i=0}^{d-1} \lambda_i |i\rangle_A \otimes |i\rangle_B \tag{2.33}$$

where $\{|i\rangle\}$ is the computational basis (2.3) such that $\lambda_i > 0$ and $\sum_i \lambda_i^2 = 1$. For a note, any pure entangled bipartite state of local dimension d can be written as (2.33) up to some local unitary transformation. The local quantum state corresponding to the subsystem ρ_A and ρ_B are given by

$$\rho_A = \sum_i \lambda_i^2 |i\rangle\langle i|_A, \quad \text{and} \quad \rho_B = \sum_i \lambda_i^2 |i\rangle\langle i|_B. \tag{2.34}$$

Any mixed quantum state [cf. Def. 2] can be realised as a pure state by adding an additional ancillary system to this quantum state. This is known as Stinespring's dilation [68]. A possible purification of any mixed quantum state ρ admitting the form given in (2.5) can be written as,

$$|\psi_{mA}\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle_m \otimes |e_i\rangle_A \tag{2.35}$$

where $\{|e_i\rangle_A\}$ is an orthonormal basis over the Hilbert space of the ancillary system A. The mixed state ρ_m can be extracted from this purified state as

$$\rho_m = \mathrm{Tr}_A \left(|\psi_{mA}\rangle\langle\psi_{mA}|\right). \tag{2.36}$$

On similar lines, any POVM can be realised as a projective measurement that acts on some higher dimensional system, known as Naimark's dilation [73]. Any n-outcome POVM $M = \{E_k\}$ that acts on the Hilbert space $\mathscr{H}$ can be realised using a projective measurement Π_k and an isometry [cf. Def. 7] $V_{iso} : \mathscr{H} \to \mathscr{H} \otimes \mathscr{H}_A$ where $\mathscr{H}_A$ is some finite dimensional Hilbert space corresponding to some ancillary system A [1], [74], as

$$E_k = V_{iso}\Pi_k V_{iso}^\dagger \quad \forall k. \tag{2.37}$$

Here, the projectors Π_k are given by

$$\Pi_i = \mathbb{1}_{\mathscr{H}} \otimes |i\rangle\langle i|_A \quad \forall i \tag{2.38}$$

such that $\{|i\rangle\}$ is the computational basis and the isometry V_{iso} is given by,

$$V_{iso} = \sum_{k=1}^{n} \sqrt{E_k} \otimes |i\rangle_A. \tag{2.39}$$

This completes the introduction of basic formalism of quantum information theory that is relevant to this work. We now move on to introducing concepts more central to this thesis.

2.2 Quantum non-locality

In the seminal work [3] published in 1935, Einstein, Podolsky and Rosen (EPR) pointed out to one of the key features of quantum theory which makes it inherently different from classical physics. In this work, two spatially separated quantum systems were considered on which two parties named Alice, and Bob can perform local measurements. The joint

quantum state of both the systems were considered to be entangled. It was concluded in this work that quantum theory is incomplete. It was later hypothesised that there could exist some hidden variables that can not be directly observed but the knowledge of which would remove the paradoxes within quantum theory. In other words, these hidden variables would provide a classical explanation of the observed quantum phenomenon. In the subsequent years it was further noted by Schrödinger [49] from the EPR work, that Alice can in fact affect the quantum state of the system which is spatially separated from her by just performing measurements on her part of the system. The problem was debated upon for decades but mostly from a philosophical perspective without much consensus. We would elaborate on these ideas with details in the subsequent subsections.

The problem was revisited again by Bell in 1964 [4], [75]. With the improved tools of quantum theory, Bell was able to devise a way that can put an end to the debate whether there exist any hidden variables that can provide a classical description of quantum theory. It turned out that there exist some set of joint probabilities that Alice and Bob can observe that can not be reproduced by local hidden variables [see below]. It was later confirmed in numerous experiments such as [5]–[8], that it is indeed the case that quantum theory is intrinsically different from classical physics. This not just led to paradigm shift in foundation of physics but also led to enormous development in the newly born field of quantum information theory. We now proceed towards understanding Bell's solution to the EPR problem and the discovery of quantum non-locality also known as "Bell non-locality".

2.2.1 Bell non-locality

We begin by considering the arguments by Einstein, Podolsky and Rosen in details. Consider two parties, namely Alice and Bob in two different spatially separated labs. Each of them receive a subsystem corresponding to an entangled quantum state such that knowing the position or momentum of either of the subsystem gives the information about the position and momentum of the counterpart. Now, Alice measures the position of her subsystem and Bob measures the momentum of his subsystem. EPR argued that for each of the subsystem one has information about its position as well as momentum which was forbidden in quantum theory as position and momentum are non-commuting measurements. This led them to conclude that there is an inherent inconsistency in quantum theory and it is incomplete. They argued that such a phenomenon should not exist which seems "non-local" in the sense that one can know the state of a far away system based on the experiment done locally on its counterpart even when there is no interaction between them. Due to this, in the subsequent years it was hypothesised by physicists like Bohm and Von-Neumann that there might exist some hidden variables that would remove this

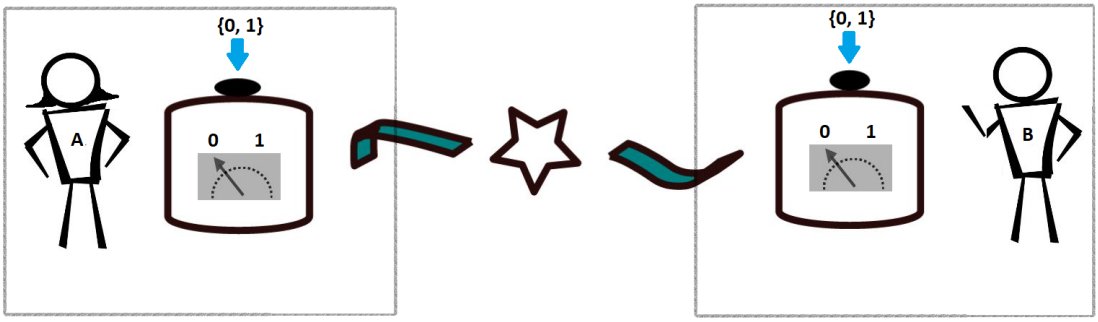


Figure 2.1: Simplest Bell scenario: Two parties Alice and Bob are located at separated labs. A source sends one subsystem to Alice and the other to Bob. Inside their labs, Alice and Bob perform two two-outcome measurements each on the received subsystem. After the experiment is complete, they compare their results to construct the joint probability distribution $p(a,b|x,y)$.

inconsistency and provide a local description of quantum theory.

Building on this idea, Bell in his original work [4] described a similar scenario. There are two parties Alice and Bob in two different labs that are spatially separated from each other. Both of them receive a quantum system from the preparation device. In their respective labs, Alice and Bob can perform two local measurements on their part of the system. During this operation they are not allowed to communicate among each other or equivalently, they are not supposed to know each others measurement choice or the outcomes of the measurements. The scenario is schematically depicted in Fig. 2.1. The experiment is repeated enough number of times to gather statistics corresponding to the joint probability distributions $\vec{p} = \{p(a,b|x,y)\}$ where $p(a,b|x,y)$ denotes the probability of obtaining outcome a,b when Alice and Bob perform x,y measurement respectively. One usually refers $\vec{p}$ as "correlations".

Let us now again consider the hypothesis that there might exist some hidden variables that would provide a consistent local description of quantum theory. Let us denote those hidden variables by λ. In presence of such hidden variables the joint probability distribution can be expressed as

$$p(a,b|x,y) = \sum_{\lambda\in\Lambda} p(a,b|x,y,\lambda)p(\lambda) \tag{2.40}$$

where Λ denotes the set of the hidden variables λ, and $p(\lambda)$ denotes the probability with which a particular λ occurs. Here, $p(a,b|x,y,\lambda)$ denotes the probability of occurrence of

outcome a,b given the input x,y and the hidden variable λ. The above statement points to the fact that we do not have access to λ and can only observe the probabilities averaged over it.

Let us now concentrate on $p(a,b|x,y,\lambda)$. From rule of conditional probabilities $p(a,b) = p(b|a)p(a)$ where $p(b|a)$ denotes the the conditional probability of occurrence of b given a, we have

$$p(a,b|x,y,\lambda) = p(a|x,\lambda)p(b|a,x,y,\lambda). \tag{2.41}$$

Now, the assumption of "locality" or "local realism" states that outcome of Bob does not depend on the outcome of Alice or her measurement choice

$$p(b|a,x,y,\lambda) = p(b|y,\lambda). \tag{2.42}$$

Thus, for any local hidden variable, we have that

$$p(a,b|x,y,\lambda) = p(a|x,\lambda)p(b|y,\lambda) \qquad \forall\lambda. \tag{2.43}$$

Consequently, any joint probability distribution admitting a local hidden variable model must be of the form

$$p(a,b|x,y) = \sum_{\lambda\in\Lambda} p(a|x,\lambda)p(b|y,\lambda)p(\lambda). \tag{2.44}$$

Now, using these joint probabilities, one can construct a functional of the form

$$\mathscr{B} = \sum_{a,b,x,y} c_{a,b,x,y}p(a,b|x,y) \tag{2.45}$$

where $c_{a,b,x,y}$ are some real numbers. For ease of understanding we refer here to a functional presented by Clauser, Horne, Shimony and Holt (CHSH) [76] in which the cofficients in (2.45) are chosen as

$$c(a,b,x,y) = \begin{cases} 1 & \text{if} \quad a\oplus_2 b = x.y \\ -1 & \text{otherwise} \end{cases} \tag{2.46}$$

where $a\oplus_2 b$ represents $a+b$ modulo 2. Usually the CHSH Bell functional is represented in the expectation value picture as

$$\mathscr{B}_{CHSH} = \langle A_0\otimes B_0\rangle + \langle A_0\otimes B_1\rangle + \langle A_1\otimes B_0\rangle - \langle A_1\otimes B_1\rangle. \tag{2.47}$$

Assuming that the joint probabilities can be described by a local hidden variable model (2.44), one arrives at an upper bound of the CHSH expression (2.47) given by

$$\mathscr{B}_{CHSH} \leq 2. \tag{2.48}$$

The maximum value that one can achieve for a Bell expression using local hidden variable models is usually referred to as the "classical bound" or the "local bound" and is denoted by β_L. It turns out that there exist some states and measurements in quantum theory that violate this bound. To give an example let us consider that the preparation device in Fig. 2.1 prepares the two-qubit maximally entangled state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right). \tag{2.49}$$

Assume then that on her share of their state Alice and Bob perform the following measurements

$$A_0 = \sigma_z \qquad \text{and} \qquad A_1 = \sigma_x, \tag{2.50}$$

and,

$$B_0 = \frac{\sigma_z + \sigma_x}{\sqrt{2}} \qquad \text{and} \qquad B_1 = \frac{\sigma_z - \sigma_x}{\sqrt{2}}. \tag{2.51}$$

respectively. It follows that for this choice of the state and measurements, the value of the CHSH expression (2.47) is

$$\mathscr{B}_{CHSH} = 2\sqrt{2}. \tag{2.52}$$

One thus concludes that there exist joint probability distributions in quantum theory that violate the notion of local realism. Contrary to EPR, Bell showed that even if there exists some hidden variables that can not be observed directly, they are insufficient to give a local explanation of some predictions of quantum theory. This is known as "Bell non-locality".

As a matter of fact, the value $2\sqrt{2}$ in Eq. (2.52) is the maximum value attainable using quantum state and measurements. This was proven by Tsirelson in [77], and is referred as "Tsirelson bound" or simply "quantum bound" and is denoted by β_Q.

An additional constraint in the above experiment as mentioned before is that there is no communication between Alice and Bob during the experiment. This restricts the joint

probability distributions to be "no-signalling" [78], that is,

$$p(a|x) = \sum_b p(a,b|x,y) = \sum_b p(a,b|x,y') \qquad \forall y,y' \tag{2.53}$$

and

$$p(b|y) = \sum_a p(a,b|x,y) = \sum_a p(a,b|x',y) \qquad \forall x,x'. \tag{2.54}$$

Assuming that the joint probability distributions are no-signalling, one can even outperform quantum theory, that is,

$$\mathscr{B}_{CHSH} = 4 \tag{2.55}$$

which is also the algebraic bound of the Bell functional $\mathscr{B}_{CHSH}$. This is also known as the "no-signalling bound" and is denoted by β_{NS}.

The above scenario can be straightforwadly generalised to the multipartite scenario where there is a preparation device, that sends subsystems to N spatially separated parties denoted by A_i for $i = 1,2,,\ldots,N$. Each of the parties can now perform $m-$measurements each of which are $d-$outcome where m,d are arbitrary positive integers strictly greater than 1. The scenario is depicted in Fig. 2.2.

The joint probability distributions in such a scenario is denoted by

$$\vec{p} = \{p(a_1,a_2,\ldots,a_N|x_1,x_2,\ldots,x_N)\}, \tag{2.56}$$

where $a_k = \{0,1,\ldots,d-1\}$ denotes the outcome when A_k performs the measurement $x_k = \{1,2,\ldots,m\}$. It is important to note here that

$$\vec{p} \in \mathbb{R}^{(md)^N}, \tag{2.57}$$

where $\mathbb{R}^{(md)^N}$ denotes the real vector space of dimension $(md)^N$. The Bell functional in the multipartite case can be written as

$$\mathscr{B}_{m,d,N} = \vec{c} \cdot \vec{p} \tag{2.58}$$

where $\vec{c} = \{c_{a_1,a_2\ldots a_N,x_1,x_2,\ldots,x_N}\}$ and $\vec{c} \in \mathbb{R}^{(md)^N}$.

The collection of joint probability distributions that admit a local hidden variable are known as the "set of local correlations" or simply "local set" denoted by $\mathscr{L}_{m,d,N}$. Similarly, one can define "set of quantum correlations" or simply "quantum set" denoted by $\mathscr{Q}_{m,d,N}$ and "set of no-signalling correlations" or "no-signalling set" denoted by $\mathscr{N}_{m,d,N}$ referring to

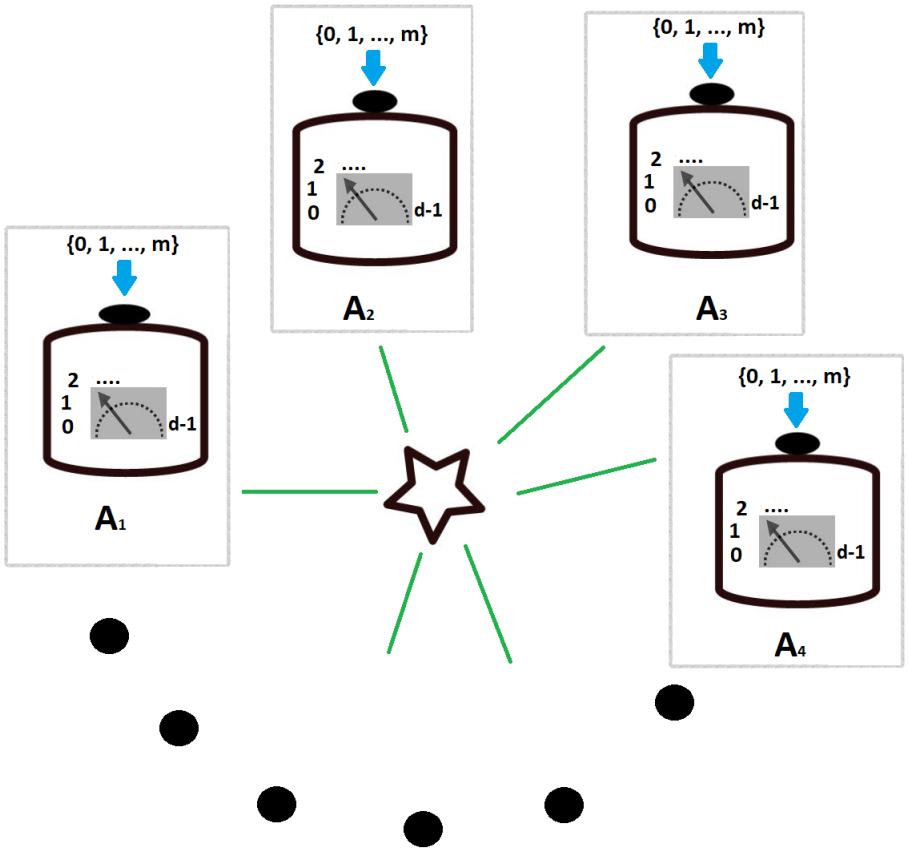


Figure 2.2: Generalised Bell scenario: N parties denoted by A_i for $i = 1,2,\ldots,N$ are located at separated labs. A source sends one subsystem to each of the labs. Inside their labs, each party performs m number of $d-$outcome measurements on the received subsystem. After the experiment is complete, they compare their results to construct the joint probability distribution $p(a_1,a_2,\ldots,a_N|x_1,x_2,\ldots,x_N)$.

joint probability distributions that admit a quantum and no-signalling models respectively. One can understand Bell's non-locality arising from the fact that the local set lies strictly inside the quantum set. All these sets are convex in nature, that is, convex combination of different elements of the set is also an element belonging to this set. Elements of the set that can not be written as a convex combination of other elements are known as "extremal points" of the set and any other element in the set can be written as a convex combination of these extremal points. By definition, the local set lies inside the quantum set that lies inside the no-signalling set [79],

$$\mathscr{L}_{m,d,N} \subseteq \mathscr{Q}_{m,d,N} \subseteq \mathscr{N}_{m,d,N}. \tag{2.59}$$

It follows from the work of Bell [4] and then Popescu and Rohrlich [78] that these inclusions

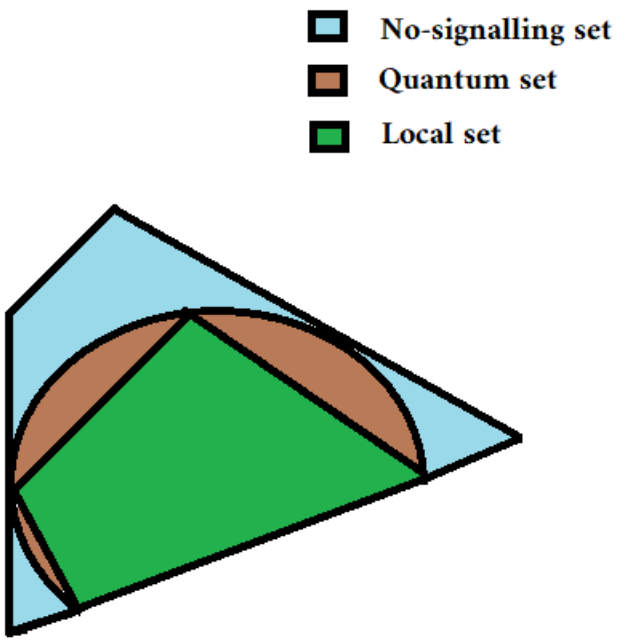


Figure 2.3: A two-dimensional representation of the set of correlations. The local set is a subset of the quantum set which is a subset of the no-signalling set. The no-signalling and local set are polytopes, that is, every point inside these sets can be written as a convex combination of the vertices of the polytope. On the other hand, the quantum set is not a polytope but convex.

are strict in the minimal scenario [m=d=N=2]. This is schematically represented in Fig. 2.3. Now, Bell inequalities can be understood as a hyper plane that cuts the quantum set into two different parts. The first part consists of correlations that admit a local model and the second part consists the rest. We now move on to a different notion of non-locality known as quantum steering.

2.2.2 Quantum steering

The idea of quantum steering was conceived by Schrödinger in 1935 but was formalised after almost 70 years in 2007 by Wisemen et. al. [50]. We begin by describing the simplest quantum steering scenario described in [80] that consits of two spatially separated parties Alice and Bob. A preparation device sends one subsystem to Alice and another subsystem to Bob. Alice sends input $y = 0, 1$ to Bob based on which Bob performs a measurement on his subsystem and gets an outcome $b = 0, 1$ which is sent back to Alice. Contrary to Bell scenario, Alice is trusted which means that Alice has full control of her lab and can

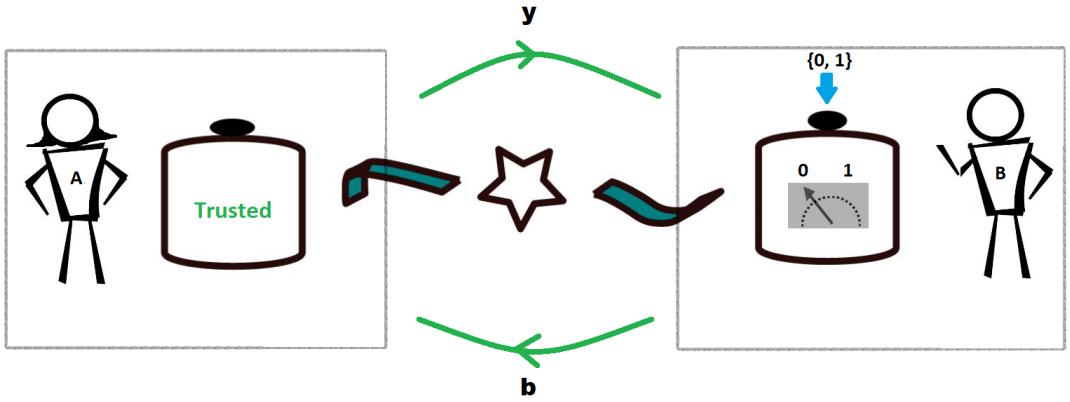


Figure 2.4: Simplest quantum steering scenario: Two parties Alice and Bob are located at separated labs. A source sends one subsystem to Alice and the other to Bob. Bob performs two two-outcome measurements on the received subsystem which might change the state of the subsystem of Alice. Alice is trusted and can perform a tomography on her subsystem and reconstruct the assemblage (the set of unnormalised states) and can figure out whether the assemblage is steerable or not.

perform a tomography on her subsystem. The experiment is repeated enough number of times such that Alice can reconstruct the state of the subsystem $\sigma_{b|y}$ that acts on Alice's Hilbert space $\mathscr{H}_A$ for every y, b. As a matter of fact these states are un-normalised and they form a set known as an assemblage, denoted by $\{\sigma_{b|y}\}$. The scenario is schematically represented in Fig. 2.4.

Similar to the idea of local hidden variables in Bell non-locality, one can define a notion which every classical description of the experiment must abide. In the quantum steering scenario presented above, the classical notion corresponds to the assemblage $\{\sigma_{b|y}\}$ admitting a local hidden state model. One can understand this as, the assemblage observed by Alice only depends on some local state ρ_λ that might be classically correlated with Bob,

$$\sigma_{b|y} = \sum_{\lambda \in \Lambda} p(\lambda) p(b|y,\lambda) \rho_\lambda . \tag{2.60}$$

Here $p(b|y,\lambda)$ represents the probability of obtaining outcome b by Bob given input y and hidden variable λ and $p(\lambda)$ denotes the probability distribution of the hidden variables. If the assemblage admits a local hidden state model then it is non-steerable from Bob to Alice. On the other hand, the assemblage is called steerable from Bob to Alice if no hidden state model can be constructed to express $\{\sigma_{b|y}\}$ as in (2.60). The way to detect

whether the assemblage is steerable or not, is to use a steering functional of the form

$$W = \sum_b \sum_y \mathrm{Tr}(F_{b|y}\sigma_{b|y}). \tag{2.61}$$

where the coefficients $F_{b|y}$ are some positive semi-definite operators acting on $\mathscr{H}_A$.

Let us now consider the first steering inequality proposed in [80]. The scenario considered there is minimal in the sense that there are only two parties and Bob performs only two measurements. The matrices $F_{b|y}$ of the steering functional were chosen as,

$$F_{0|0} = |0\rangle\langle 0|, \qquad F_{1|0} = |1\rangle\langle 1| \tag{2.62}$$

and

$$F_{0|1} = |+\rangle\langle +|, \qquad F_{1|0} = |-\rangle\langle -|, \tag{2.63}$$

where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Consequently, the simplest steering functional can be represented as

$$W_{2,2,2} = \mathrm{Tr}\left(|0\rangle\langle 0|\sigma_{0|0}\right) + \mathrm{Tr}\left(|1\rangle\langle 1|\sigma_{1|0}\right) + \mathrm{Tr}\left(|+\rangle\langle +|\sigma_{0|1}\right) + \mathrm{Tr}\left(|-\rangle\langle -|\sigma_{1|1}\right). \tag{2.64}$$

For assemblages that admit a local hidden state model, one can find an upper bound to the steering functional (2.61) as

$$W_{2,2,2} \leq 1 + \frac{1}{\sqrt{2}}. \tag{2.65}$$

This is known as "local hidden state bound" or simply "local bound" and is again denoted by β_L. The quantum bound β_Q of the steering inequality $W_{2,2,2}$ is 2 and for instance can be achieved when the preparation device prepares the maximally entangled state (2.49) and Bob performs the Pauli z and Pauli x measurements

$$B_0 = \sigma_z, \qquad B_1 = \sigma_x. \tag{2.66}$$

The scenario can be straightforwardly generalised to the case when Bob performs arbitrary number of measurements m with arbitrary number of outcomes d. The steering functional in this case admits a form

$$W_{m,d,2} = \sum_{y=1}^{m} \sum_{b=0}^{d-1} \mathrm{Tr}(F_{b|y}\sigma_{b|y}). \tag{2.67}$$

Comparing Bell scenario to quantum steering scenario, in Bell scenario one obtains joint

probability distributions from the experiment and constructs the Bell functional by suitably choosing the real coefficients $c_{a,b,x,y}$. In quantum steering scenario the experiment generates the assemblage and the steering functional is constructed by suitably choosing the positive semi-definite matrices $F_{b|y}$. However, it is always possible to map quantum steering to the Bell scenario and express the steering functional in terms of expectation values of joint observables or equivalently joint probability distributions $\vec{p}$ similar to Bell functional. This idea will be particularly useful for this thesis.

Let us consider the steering functional $W_{m,d,2}$ (2.67) with the coefficients $F_{b|y}$ being positive, Hermitian and summing up to the identity for all y, that is,

$$F_{b|y} \geq 0, \qquad F_{b|y} = F_{b|y}^{\dagger}, \qquad \sum_{b} F_{b|y} = \mathbb{1}. \tag{2.68}$$

Consequently, $\{F_{b|y}\}$ is a valid quantum measurement. As discussed in subsection 2.1.3, one can equivalently represent a quantum measurement by using d generalised observables $A_{k|y}$ (2.21), that is,

$$F_{b|y} = \frac{1}{d} \sum_{b=0}^{d-1} \omega^{-bk} A_{k|y} \tag{2.69}$$

with $k = 0, \ldots, d-1$ and $\omega = \exp(2\pi i/d)$. Let us now consider that Bob performs the measurements $\{N_{b|y}\}$ on some state ρ_{AB}. Then, the assemblage $\sigma_{b|y}$ can be expressed as

$$\sigma_{b|y} = \mathrm{Tr}_B[(\mathbb{1}_A \otimes N_{b|y})\rho_{AB}]. \tag{2.70}$$

Again, we represent the measurements $\{N_{b|y}\}$ using d generalised observables $B_{l|y}$ as

$$N_{b|y} = \frac{1}{d} \sum_{b=0}^{d-1} \omega^{-bl} B_{l|y}. \tag{2.71}$$

Now, we are ready to express the steering functional (2.67) in terms of expectation values. First using the observation (2.70), the steering functional (2.67) can be written as

$$\begin{aligned} W_{m,d,2} &= \sum_{b} \sum_{y} \mathrm{Tr}(F_{b|y} \sigma_{b|y}) \\ &= \sum_{b} \sum_{y} \mathrm{Tr}(F_{b|y} \otimes N_{b|y} \rho_{AB}). \end{aligned} \tag{2.72}$$

Now, using observations (2.69) and (2.71), we arrive at

$$\sum_{b=0}^{d-1} \sum_{y=1}^{N} \mathrm{Tr}(F_{b|y} \sigma_{b|y}) = \frac{1}{d} \sum_{k=0}^{d-1} \sum_{y=1}^{N} \left\langle A_{k|y} \otimes B_{-k|y} \right\rangle. \tag{2.73}$$

For a detailed review on quantum steering, refer to [81]. In the next part, we briefly discuss the applications of quantum non-locality.

2.2.3 Applications of quantum non-locality

Apart from the foundational aspects, quantum non-locality has has given rise to enormous number of applications in computation, communication and information theory. Here we first give a brief account of various applications of Bell non-locality and then quantum steering.

Suppose, Alice and Bob are spatially separated and both of them receive $n-$bit strings denoted by x,y and Bob wants to compute a function $f(x,y)$. The minimum amount of information needed by Bob from Alice to compute $f(x,y)$ is known as communication complexity of $f(x,y)$. It has been shown that for certain functions $f(x,y)$, Bell non-locality reduces the communication complexity when compared to classical communication between Alice and Bob [82]. Another important application of Bell-nonlocality is in the field of quantum cryptography. The earliest connection between quantum non-locality and cryptography was realised by Herbert in 1975 [83]. However, the breakthrough was achieved by Ekert in his seminal paper in 1991 [84] that showed that Bell-nonlocality serves as a way to generate secure key among two spatially separated parties. The protocol was based on the maximal violation of CHSH inequality which makes it physically impossible for some external attacker to know the key shared between Alice and Bob. As a consequence this protocol can be realised in a device-independent way, that is, without assuming any details about the inner working of the device apart from the fact that it is governed by quantum theory. In fact device-independent quantum key distribution (DIQKD) has been one of the key applications of quantum non-locality [9], [63], [85]–[93]. Using Bell inequalities one can even find the minimum dimension of a quantum system required for obtaining certain correlations [94]. Since Bell inequalities can be violated using only entangled states, they serve as an important tool to detect entanglement [95]–[98]. Bell non-locality has been identified as a way to generate genuine randomness [41], [64], [65], [99]–[110].

Mayers and Yao in [10], [11] realised that correlations obtained by performing local measurements on spatially separated systems can used for device-independent certification of quantum states and measurements. This was termed as self-testing. It was later realised that in fact Bell-nonlocality allows one to self-test quantum states and measurements [12], [13], [16], [22], [23], [32], [43], [45]. In the subsequent sections, we discuss device-independent certification and randomness generation in details.

Quantum steering is also useful in quantum cryptography as was realised in [111], [112]. In a practical scenario where one of the parties is trusted, for instance, in a bank-

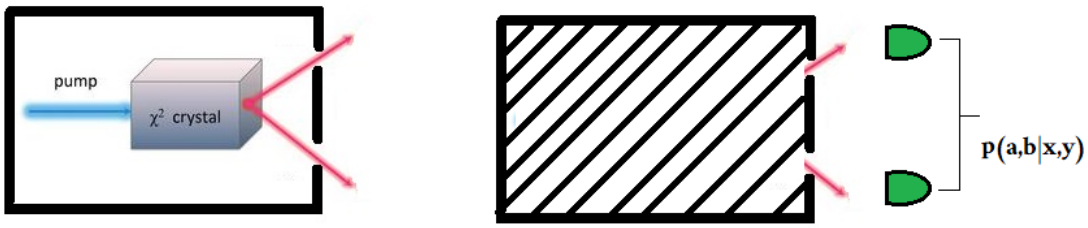
client relationship where the bank can be considered to be trusted, one can construct one-sided device-independent protocols. Since, then there have been numerous protocols for quantum key distribution using quantum steering [113]–[117]. Quantum steering is also useful in tasks like secret sharing, where a referee sends an encrypted message to multiple players which can be decoded only if the players work together [118]–[121]. Also, randomness can be certified using quantum steering to be secure and genuine [122]–[125]. Quantum steering has also shown advantage in tasks like subchannel discrimination, that is, how well one can distinguish different branches of a quantum channel [126], [127]. Further, quantum steering can be used for certification of quantum states and measurements [51], [52], [128], [129].

This completes the analysis of quantum non-locality relevant to this thesis. In the next section we introduce the idea of device-independent certification and in particular self-testing and one-sided device certification.

2.3 Device-independent certification

In recent years, the field of device-independent schemes has gained a lot of interest. The novelty of such schemes lies in the fact that one can predict some properties about the system by looking only at the statistics generated by this system. For instance, consider that we are given a device that is promised to produce entangled photons. The natural question is how we verify that the device works as promised and whether we should trust the manufacturer. One way is to break the device and check the source. Another way is not to break the device but perform a quantum tomography on the state generated by the device. But one needs the knowledge of quantum optics and also would have to trust his measurement device to infer the state. However, using Bell inequalities, we can verify the device without breaking it or without trusting any other device. For this, as depicted in Fig. 2.5, the entangled subsystems are allowed to be far enough such that they are spatially separated. Now, two local measurements are performed on each of these arms. Here the verifiers do not have any knowledge about the measurement device but choose two inputs freely corresponding to the two measurements and record their outputs. The experiment is repeated enough number of times to collect joint probability distribution for different inputs and outputs. If this distribution violates some Bell inequality, it can be concluded that the device generates entangled photons.

Thus, quantum nonlocality serves as a way to infer properties about a device without knowing the inner workings of it apart from the fact that it is governed by quantum theory. Such device-independent schemes provide maximum security in cryptographic scenarios where there might be some hidden mechanisms that are uncontrollable or the



(a) (b)

Figure 2.5: (a) Device-dependent scenario: To verify the device, one has to assume the inner workings of the device. Here, if it is known that the device consists a photon source that passes through a χ^2 crystal, then the device can produce entangled photons. (b) Device-independent scenario: The inner workings of the device are unknown. To verify whether the device generates entangled photons, one needs to perform a Bell test by measuring the joint correlation statistics $p(a,b|x,y)$.

device leaks out some information that can be used by some external attacker. However, in practical scenarios one can make some well justified assumptions on the device. In this thesis, we focus on two different types of device-independent certification, first, fully device-independent certification or self-testing and second, one-sided device independent certification.

2.3.1 Self-testing

Let us now consider the following task: Instead of detecting some property about the state such as entanglement, we want to characterise the state and measurement which generates the observed statistics with the device being treated as a black box. This is the strongest form of device-independent certification and is known as self-testing. The idea of fully device-independent certification or self-testing was first introduced by Mayers and Yao in 1998 [10], [11]. The scenario for self-testing is same as Bell scenario Fig. 2.1. There are two independent observers Alice and Bob who are spatially separated from each other and can freely choose their inputs. Also, they are not allowed to communicate among each other during the experiment. However, the natural assumption here is that the device behaves according to quantum theory, that is, every statistics is generated by some quantum measurement acting on some quantum state. Another important assumption here is that the preparation device always prepares the same state and there is no correlation between the measurement device and the preparation device. From the experiment Alice and Bob obtain the joint probability distribution $\{p(a,b|x,y)\}$ where a,b denote the outcomes when they choose the measurements labelled by x,y, respectively.

Now, consider that the preparation device generates the state ρ and the measurements performed by Alice and Bob in the observable picture as $A_{a|x}$ and $B_{b|y}$ [see Sec. 2.1.3]

respectively for all a,b,x,y. For simplicity, from here on we refer the observables $A_{a|x}$ and $B_{b|y}$ as measurements. Using the joint probability distribution $\{p(a,b|x,y)\}$, Alice and Bob want to characterise the state ρ sent by the preparation device and also their measurements represented in the observable picture as $A_{a|x}$ and $B_{b|y}$ for all a,b,x,y. It is important here to note that one can identify such quantum realisations only up to the equivalences under which the probability distribution remains invariant. Also, notice that in the scenario presented above, one can not certify the source to be producing a unique mixed state. The reason being that any mixed state can be decomposed in terms of pure states. Let us say that the target or the ideal state that is expected to be produced by the source is denoted by $|\tilde{\psi}\rangle$ and the target measurements that are expected to be performed are denoted in the observable form as $\tilde{A}_{a|x}$ for Alice and $\tilde{B}_{b|y}$ for Bob. Then, there are two major equivalences under which the probability remains invariant,

1. An additional state might be attached to the target state on which the measurements act trivially, that is, the actual state and measurements in the device can be

$$\rho = |\tilde{\psi}\rangle\langle\tilde{\psi}| \otimes \sigma \tag{2.74}$$

such that σ acts on some unknown but finite dimensional Hilbert space $\mathscr{H}''$ and,

$$A_{a|x} = \tilde{A}_{a|x} \otimes \mathbb{1}'' \quad B_{b|y} = \tilde{B}_{b|y} \otimes \mathbb{1}''. \tag{2.75}$$

2. The actual state and measurements might be unitarily rotated with respect to the target state, that is,

$$\rho = U_A \otimes U_B \ |\tilde{\psi}\rangle\langle\tilde{\psi}| \ U_A^\dagger \otimes U_B^\dagger, \tag{2.76}$$

and

$$A_{a|x} = U_A \tilde{A}_{a|x} U_A^\dagger, \quad B_{b|y} = U_B \tilde{B}_{b|y} U_B^\dagger \tag{2.77}$$

where $U_A : \mathscr{H}_A \to \mathscr{H}_A$, $U_B : \mathscr{H}_B \to \mathscr{H}_B$ are local unitary transformations on the subsystem of Alice and Bob respectively.

Given these two equivalences, we now present the self-testing definition that is relevant for this thesis.

Definition 10 (Self-testing)**.** *Consider the above Bell experiment with Alice and Bob performing measurements $A_{a|x}$ and $B_{b|y}$ on a state ρ_{AB} and observing correlations $\{p(a,b|x,y)\}$. The state ρ_{AB} and measurements $A_{a|x}$ and $B_{b|y}$ are certified to be the target state $|\tilde{\psi}\rangle$ and target measurements $\tilde{A}_{a|x}$ and $\tilde{B}_{b|y}$ from $\{p(a,b|x,y)\}$ if:*

1. *The Hilbert space of Alice and Bob decompose as*

$$\mathscr{H}_A = \mathscr{H}_{A'} \otimes \mathscr{H}_{A''}, \qquad \mathscr{H}_B = \mathscr{H}_{B'} \otimes \mathscr{H}_{B''} \tag{2.78}$$

where the target state $|\tilde{\psi}\rangle$ *belongs to* $\mathscr{H}_{A'} \otimes \mathscr{H}_{B'}$ *and* $\mathscr{H}_{A''}$ *and* $\mathscr{H}_{B''}$ *represents the auxiliary Hilbert space of Alice and Bob respectively.*

2. *There exists a unitary* $U_B : \mathscr{H}_B \to \mathscr{H}_B$ *and* $U_A : \mathscr{H}_A \to \mathscr{H}_A$ *such that the state is*

$$U_A \otimes U_B \ \rho_{AB} \ U_A^\dagger \otimes U_B^\dagger = |\tilde{\psi}\rangle\langle\tilde{\psi}|_{A'B'} \otimes \sigma_{A''B''}, \tag{2.79}$$

where $\sigma_{A''B''}$ *is some state acting on the Hilbert space* $\mathscr{H}_{A''} \otimes \mathscr{H}_{B''}$.

3. *The measurements are certified as*

$$U_A A_{a|x} U_A^\dagger = \tilde{A}_{a|x} \otimes \mathbb{1}_{A''}, \qquad U_B B_{b|y} U_B^\dagger = \tilde{B}_{b|y} \otimes \mathbb{1}_{B''}. \tag{2.80}$$

for all a,b,x,y. *Here,* $\mathbb{1}_{A''}, \mathbb{1}_{B''}$ *are identities acting on the Hilbert space* $\mathscr{H}_{A''}$ *and* $\mathscr{H}_{B''}$ *respectively.*

One natural assumption that we make in the above definition is that the local states of Alice and Bob are full-rank. This comes from the fact that Alice and Bob can only characterise the part of the quantum measurements that act on the quantum state. Notice, that in general the unitaries appearing in the second equivalence can be replaced by isometries [see Def. 7]. Another important equivalence pointed out in [130], that is not stated above is that the actual quantum state and measurements can not be distinguished from the conjugate of the target state and measurements, that is,

$$\rho = |\tilde{\psi}\rangle\langle\tilde{\psi}|^*, \quad A_{a|x} = \tilde{A}^*_{a|x}, \quad B_{b|y} = \tilde{B}^*_{b|y}. \tag{2.81}$$

However, this equivalence is not relevant for this thesis (it will be clarified when analysing the results of this thesis). For other definitions of self-testing refer to [131].

As discussed before, the set of joint probability distributions is convex. It is important to note here that one can only certify quantum states and measurements from probability distribution that lie at the boundary of this set, that is, extremal probability distributions [132]. The reason is that any point inside this set can be represented as convex combination of the extremal points which does not correspond to a unique probability distribution and thus can not be achieved by only a particular state and measurements.

Now, It turns out that if one utilises the maximal violation of the Bell inequalities, then the desired self-testing of quantum state and measurements can be achieved by collecting less statistics compared to the case when one uses tomography. For instance, both Alice

and Bob are required to choose at least four inputs corresponding to a tomographically complete set of measurements to certify any two qubit state. However, employing Bell inequalities one can certify two qubit states using only two measurements per party. The maximal violation of a Bell inequality is achieved by the joint probability distributions lying at the boundary of the quantum set as shown in Fig. 2.6. However, it might happen that the Bell functional touches the boundary of the quantum set at more than one point and one can have some weaker self-testing statement where one certifies a family of states or measurements [133]–[135]. To certify some particular quantum state and measurements, the Bell violation should point to a unique probability distribution. As a consequence, to self-test any quantum realisation, we need to ensure the maximum violation of the Bell inequality and then we need to show that the probability distribution that gives the maximum violation is generated by unique quantum state and measurements up to the equivalences as suggested before. Thus, in the definition of self-testing [cf. Def. 10], we can replace the statement "observing correlations $\{p(a,b|x,y)\}$" with "observing the maximal violation of a Bell inequality $\mathscr{B}$".

In a physical experiment, we can never achieve the maximal violation of a Bell inequality but some value which is close to this violation. From an experimental perspective, it is thus necessary to understand self-testing in the presence of noise and whether the proposed certification schemes are robust against experimental imperfections.

Definition 11 (Robust self-testing)**.** *Consider the above Bell experiment with Alice and Bob performing the measurements $A_{a|x}$ and $B_{b|y}$ respectively on a quantum state ρ_{AB}. Assume that the value of a given Bell expression $\mathscr{B}$ for the observed correlations satisfy*

$$\mathscr{B} \geq \beta_Q - \varepsilon. \tag{2.82}$$

Alice and Bob can robustly certify a target state $|\tilde{\psi}\rangle$ and target measurements $\tilde{A}_{a|x}$ and $\tilde{B}_{b|y}$ from the observed Bell value, if there exists a unitary $U_B : \mathscr{H}_B \to \mathscr{H}_B$ and $U_A : \mathscr{H}_A \to \mathscr{H}_A$ such that the state is

$$\left|\left| U_A \otimes U_B \rho_{AB} U_A^\dagger \otimes U_B^\dagger - |\tilde{\psi}\rangle\langle\tilde{\psi}|_{A'B'} \otimes \sigma_{A''B''} \right|\right|_2 \leq f_1(\varepsilon), \tag{2.83}$$

where $\sigma_{A''B''}$ is some state acting on the Hilbert space $\mathscr{H}_{A''} \otimes \mathscr{H}_{B''}$ and the measurements are

$$\begin{aligned} ||U_A A_{a|x} U_A^\dagger - \tilde{A}_{a|x} \otimes \mathbb{1}_{A''}||_2 &\leq f_2(\varepsilon), \quad \text{and} \\ ||U_B B_{b|y} U_B^\dagger - \tilde{B}_{b|y} \otimes \mathbb{1}_{B''}||_2 &\leq f_3(\varepsilon). \end{aligned} \tag{2.84}$$

for all a,b,x,y and $\mathbb{1}_{A''}, \mathbb{1}_{B''}$ are identities acting on to the support of Alice's and Bob's

subsystem ρ_A, ρ_B *respectively. Further, when* ε *goes to* 0*, the functions* $f_1(\varepsilon), f_2(\varepsilon)$ *and* $f_3(\varepsilon)$ *must vanish.*

For a note, the $||X||_2$ denotes the Hilbert-Schmidt norm of an operator X, and is defined as $||X||_2 = \sqrt{\text{Tr}(X^\dagger X)}$. For two unitary matrices A and $\tilde{A}$, we have that

$$||A - \tilde{A}||_2 = 2\left[\text{Tr}(\mathbb{1}) - \text{ReTr}(A\tilde{A}^\dagger)\right]. \tag{2.85}$$

The above statement can be understood as, if one observes a value ε lower than the maximal violation in a Bell experiment, then overlap between the state shared between the parties and the target state up to some equivalences is bounded from below by a function of ε. One can arrive at a similar conclusion for the measurements.

Ways to do self-testing

There are several works that provide self-testing statements using numerical approaches based on semi-definite programs [27], [28], [34], [35]. However, these methods can not be used to provide self-testing statements for higher dimensional states due to computational requirements. In other words, there does not exist any numerical scheme that can certify entangled states of arbitrary local dimension in an efficient way. Due to this, in this work we focus on analytical methods of self-testing.

There are a few analytical techniques that have been explored for the task of self-testing but most of these techniques work when the state to be certified is a two-qubit state. For instance, the initial self-testing schemes [21], [23], [30] were based on Jordan's lemma [63], [136] that says that if two Hermitian matrices with eigenvalues ± 1 act on a Hilbert space $\mathscr{H}$, then these matrices decompose as a direct sum of matrices acting on Hilbert space of dimension less than or equal to two. Another such method is using the swap gate that serves as an isometry that maps the non-ideal state to the target state [12], [13], [15], [16], [25], [32].

In this thesis, we follow another approach to derive self-testing statements that is based on "sum of squares (SOS) decomposition" of the Bell operator. This involves decomposing the Bell operator in terms of some positive operators. This method was first explored for self-testing of any pure entangled two-qubit state in [14]. Based on this method, some self-testing schemes were provided in [24], [41], [133] that can be used to certify multi-qubit states and subspaces. A scheme to self-test two-qutrit maximally entangled state was proposed in [31] that employed the method of SOS decomposition of the Bell operator. In [31], [39] family of Bell inequalities were constructed using this technique, the maximal violation of which was achieved by maximally entangled state of arbitrary local dimension.

Let us now elaborate on the SOS decomposition of a Bell operator. Any Bell operator

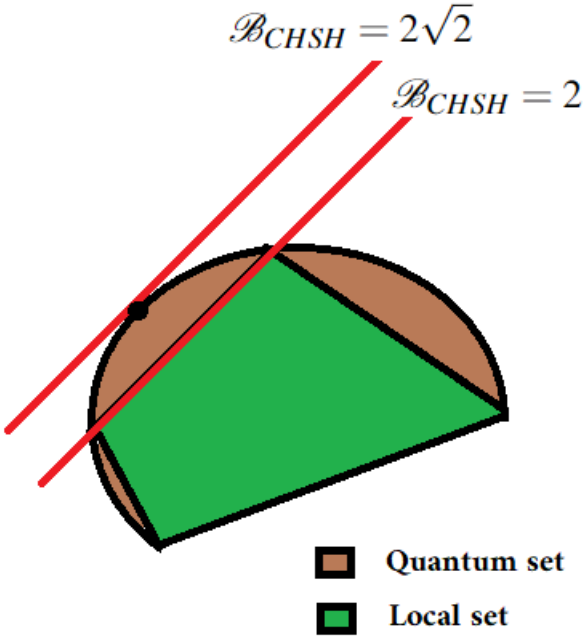


Figure 2.6: The CHSH functional $\mathscr{B}_{CHSH} = 2$ represents a facet of the local set of correlations $\mathscr{L}_{2,2,2}$. In other words, CHSH functional is a hyperplane that represents one of the face of the local polytope. Interestingly, the CHSH functional $\mathscr{B}_{CHSH} = 2\sqrt{2}$ touches the quantum set at a single extremal point making it particularly useful for self-testing.

(2.45) can be represented as

$$\hat{\mathscr{B}} = \sum_{a,b,x,y} c_{a,b,x,y} M_{a|x} \otimes N_{b|y} \tag{2.86}$$

where $M_{a|x}, N_{b|y}$ are measurement operators corresponding to the input x and output a of Alice and input y and output b of Bob respectively. If β_Q is the quantum bound of the Bell expression $\langle \hat{\mathscr{B}} \rangle$ where $\hat{\mathscr{B}}$ is given in (2.86), then let us assume that the positive semi-definite operator $\beta_Q \mathbb{1} - \hat{\mathscr{B}}$ can be decomposed in the following way

$$\beta_Q \mathbb{1} - \hat{\mathscr{B}} = \sum_i P_i^\dagger P_i. \tag{2.87}$$

Note that the right hand side of the above equation consists of positive operators $P_i^\dagger P_i$ composed of the operators $M_{a|x}, N_{b|y}$. Given a generic Bell operator, it is not that straightforward to find such decompositions. One can numerically find it using the Navascués-Pironio-Acín (NPA) hierarchy [137]–[139] which is based on semi-definite programming. Let us now consider that the state $|\psi\rangle$ achieves the maximal violation of a Bell inequality,

then the left hand side of (2.87) vanishes and thus

$$\sum_i ||P_i|\psi\rangle||^2 = 0. \tag{2.88}$$

All the terms are positive in the above sum which allows to conclude that $||P_i|\psi\rangle|| = 0$ for all i. Thus,

$$\forall i \qquad P_i|\psi\rangle = 0. \tag{2.89}$$

This simple expression contains all the information about the state and measurements that give rise to the maximal violation of the corresponding Bell inequality. Often, these relations can be used to derive self-testing results.

Since, this technique is central to the results presented in this thesis we would provide a simple example of self-testing based on SOS decomposition. Before proceeding let us state an important fact that was proven in Ref. [31] which is central to some of the results presented in this thesis.

Fact 2. *Consider two unitary matrices R_0, R_1 that act on a finite-dimensional Hilbert space $\mathscr{H}$ satisfying $R_0^d = R_1^d = \mathbb{1}$. If R_0 and R_1 satisfy the relation $R_0R_1 = \omega R_1R_0$, then $dim(\mathscr{H}) = d.t$ for some positive integer t and there exists a unitary $U : \mathscr{H} \to \mathscr{H}$ such that*

$$UR_0U^\dagger = Z_d \otimes \mathbb{1}, \quad \text{and} \quad UR_1U^\dagger = X_d \otimes \mathbb{1}, \tag{2.90}$$

where Z_d, X_d are the $d-$dimensional generalisation of the Pauli matrices σ_z, σ_x (2.27) given by,

$$Z_d = \sum_{i=0}^{d-1} \omega^i |i\rangle\langle i|, \qquad X_d = \sum_{i=0}^{d-1} |i+1\rangle\langle i|. \tag{2.91}$$

Let us now consider the CHSH inequality (2.47), which for our convenience is scaled down by the factor $\frac{1}{\sqrt{2}}$, and consider its operator form

$$\hat{\mathscr{B}}_{CHSH} = \frac{1}{\sqrt{2}} \left(A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1\right). \tag{2.92}$$

We assume here that the measurements of Alice and Bob are projective and thus, $A_x^2 = B_y^2 = \mathbb{1}$ for all x, y. The local and quantum bound of this Bell inequality is $\sqrt{2}$ and 2 respectively (2.52) and thus the SOS decomposition of the corresponding shifted Bell

operator is given by

$$2\mathbb{1} - \hat{\mathscr{B}}_{CHSH} = \frac{1}{2}\left(P_0^\dagger P_0 + P_1^\dagger P_1\right) \tag{2.93}$$

where,

$$P_0 = \mathbb{1} - A_0 \otimes \frac{B_0 + B_1}{\sqrt{2}} \quad \text{and} \quad P_1 = \mathbb{1} - A_1 \otimes \frac{(B_0 - B_1)}{\sqrt{2}}. \tag{2.94}$$

Let us now suppose that a state ρ_{AB} attains the quantum bound of the above Bell operator. Then, we can always add an ancillary system E to purify this state. Let us denote this purified state by $|\psi_{ABE}\rangle$ such that $\rho_{AB} = \mathrm{Tr}_E(|\psi\rangle\langle\psi|_{ABE})$. Then, from Eq. (2.94) the following relations must hold,

$$\left[A_0 \otimes \frac{B_0 + B_1}{\sqrt{2}} \otimes \mathbb{1}_E\right] |\psi_{ABE}\rangle = |\psi_{ABE}\rangle \tag{2.95}$$

and,

$$\left[A_1 \otimes \frac{B_0 - B_1}{\sqrt{2}} \otimes \mathbb{1}_E\right] |\psi_{ABE}\rangle = |\psi_{ABE}\rangle \tag{2.96}$$

Using the fact that A_0 are unitary and Hermitian, we have from Eq. (2.95) that

$$\frac{B_0 + B_1}{\sqrt{2}} \otimes \mathbb{1}_{AE} |\psi_{ABE}\rangle = A_0 \otimes \mathbb{1}_{BE} |\psi_{ABE}\rangle \tag{2.97}$$

Let us recall that the measurements can be characterised only on the support of the local reduced states ρ_A and ρ_B and consequently, in the proof we assume that the local states of Alice and Bob are full-rank. Also, From here on, for convenience we drop the term $\mathbb{1}_E$. Now, multiplying by $A_0 \otimes \mathbb{1}_B$ on both the sides of Eq. (2.97) , we have that

$$\left[\mathbb{1}_A \otimes \frac{B_0 + B_1}{\sqrt{2}}\right] A_0 \otimes \mathbb{1}_B |\psi_{ABE}\rangle = A_0^2 \otimes \mathbb{1}_B |\psi_{ABE}\rangle \tag{2.98}$$

where we used the fact that measurements acting on subsystem A and B commute. Using (2.97) and the fact that $A_0^2 = \mathbb{1}$, we have that

$$\mathbb{1} \otimes \left[\frac{B_0 + B_1}{\sqrt{2}}\right]^2 |\psi_{ABE}\rangle = |\psi_{ABE}\rangle. \tag{2.99}$$

Taking a partial trace over the subsystems A, E, we have that

$$\left[\frac{B_0 + B_1}{\sqrt{2}}\right]^2 \rho_B = \rho_B. \tag{2.100}$$

The fact that ρ_B is full-rank and thus invertible allows us to conclude from the above equation that

$$\left[\frac{B_0 + B_1}{\sqrt{2}}\right]^2 = \mathbb{1}_B. \tag{2.101}$$

Similarly, one obtains from (2.96) that

$$\left[\frac{B_0 - B_1}{\sqrt{2}}\right]^2 = \mathbb{1}_B. \tag{2.102}$$

Expanding the the above two equations (2.101) and (2.102), we have that

$$B_0^2 + B_1^2 + \{B_0, B_1\} = 2\mathbb{1}_B, \quad \text{and} \quad B_0^2 + B_1^2 - \{B_0, B_1\} = 2\mathbb{1}_B \tag{2.103}$$

where $\{B_0, B_1\} = B_0 B_1 + B_1 B_0$ denotes the anti-commutator of B_0, B_1. Now, using the fact that $B_0^2 = B_1^2 = \mathbb{1}_B$, we obtain that

$$\{B_0, B_1\} = 0. \tag{2.104}$$

Now, as stated in Fact 2, for two unitary matrices B_0, B_1 with the additional property that $B_i^2 = \mathbb{1}_B$ for $i = 0, 1$ and satisfy the condition (2.104), there exist local unitary transformation $V_B : \mathscr{H}_B \to \mathscr{H}_B$ such that

$$V_B \; B_0 \; V_B^\dagger = \sigma_z \otimes \mathbb{1}_{B''}, \quad \text{and} \quad V_B \; B_1 \; V_B^\dagger = \sigma_x \otimes \mathbb{1}_{B''} \tag{2.105}$$

where $\mathbb{1}_{B''}$ acts on the auxiliary Hilbert space $\mathscr{H}_{B''}$ of some finite dimension and σ_z, σ_x are Pauli matrices (2.27). This also shows that the Hilbert space of Bob decomposes as $\mathscr{H}_B = \mathbb{C}^2 \otimes \mathscr{H}_{B''}$. Now, consider a unitary matrix $W = W' \otimes \mathbb{1}_{B''}$ such that W' is also unitary and can be expressed as a matrix written in the $2-$dimensional computational basis $\{|0\rangle, |1\rangle\}$ as

$$W' = \begin{pmatrix} \cos\left(\frac{\pi}{8}\right) & \sin\left(\frac{\pi}{8}\right) \\ \sin\left(\frac{\pi}{8}\right) & -\cos\left(\frac{\pi}{8}\right) \end{pmatrix}. \tag{2.106}$$

The unitary matrix W' transforms the Pauli observables σ_z, σ_x to the ideal ones (2.51)

and thus from Eq. (2.105) we arrive at

$$U_B B_0 U_B^\dagger = \frac{\sigma_z + \sigma_x}{\sqrt{2}} \otimes \mathbb{1}_{B''} \qquad \text{and} \qquad U_B B_1 U_B^\dagger = \frac{\sigma_z - \sigma_x}{\sqrt{2}} \otimes \mathbb{1}_{B''}, \tag{2.107}$$

where $U_B = W V_B$. Now, to find Alice's observables A_i we consider an analogous SOS decomposition of the CHSH operator given by

$$2\mathbb{1} - \hat{\mathscr{B}}_{CHSH} = \frac{1}{2}\left(Q_0^\dagger Q_0 + Q_1^\dagger Q_1\right) \tag{2.108}$$

where,

$$Q_0 = \mathbb{1} - \frac{A_0 + A_1}{\sqrt{2}} \otimes B_0 \quad \text{and} \quad Q_1 = \mathbb{1} - \frac{A_0 - A_1}{\sqrt{2}} \otimes B_1. \tag{2.109}$$

Again, for any state $|\psi_{ABE}\rangle$ that maximally violates the CHSH inequality, from Eq. (2.109) the following relations must hold,

$$\frac{A_0 + A_1}{\sqrt{2}} \otimes B_0 \otimes \mathbb{1}_E |\psi_{ABE}\rangle = |\psi_{ABE}\rangle \tag{2.110}$$

and

$$\frac{A_0 - A_1}{\sqrt{2}} \otimes B_1 \otimes \mathbb{1}_E |\psi_{ABE}\rangle = |\psi_{ABE}\rangle. \tag{2.111}$$

As concluded for Bob's observables, the Hilbert space of Alice decomposes as $\mathscr{H}_A = \mathbb{C}^2 \otimes \mathscr{H}_{A''}$ and there exist local unitary transformation $U_A : \mathscr{H}_A \to \mathscr{H}_A$ such that

$$U_A\, A_0\, U_A^\dagger = \sigma_z \otimes \mathbb{1}_{A''}, \quad \text{and} \quad U_A\, A_1\, U_A^\dagger = \sigma_x \otimes \mathbb{1}_{A''} \tag{2.112}$$

where $\mathbb{1}_{A''}$ acts on the auxiliary Hilbert space $\mathscr{H}_{A''}$.

After determining the form of the measurements, we can finally certify the quantum state $|\psi_{ABE}\rangle$ that achieves the maximum violation of the CHSH Bell inequality. Since, $\mathscr{H}_A = \mathbb{C}^2 \otimes \mathscr{H}_{A''}$ and $\mathscr{H}_B = \mathbb{C}^2 \otimes \mathscr{H}_{B''}$, we can decompose the state $|\psi_{ABE}\rangle$ as

$$U_A \otimes U_B |\psi_{ABE}\rangle = |\tilde{\psi}_{ABE}\rangle = \sum_{i,j=0,1} |i\rangle_{A'} |j\rangle_{B'} |\psi_{ij}\rangle_{A''B''E} \tag{2.113}$$

where $|\psi_{ij}\rangle_{A''B''E} \in \mathscr{H}_{A''} \otimes \mathscr{H}_{B''} \otimes \mathscr{H}_E$. For convenience, we drop the subscripts from the state. Now, plugging in the certified measurements (2.107) and (2.112) in the SOS relation (2.95)

$$\sigma_z \otimes \sigma_z \otimes \mathbb{1}_{A''B''E} |\tilde{\psi}_{ABE}\rangle = |\tilde{\psi}_{ABE}\rangle. \tag{2.114}$$

Substituting the general form of the state (2.113) and simplifying, we obtain that

$$\sum_{i,j=0,1} (-1)^{ij} |i\rangle_{A'} |j\rangle_{B'} |\psi_{ij}\rangle_{A''B''E} = \sum_{i,j=0,1} |i\rangle_{A'} |j\rangle_{B'} |\psi_{ij}\rangle_{A''B''E}. \tag{2.115}$$

By projecting the above equation on to $\langle i|_{A'} \langle j|_{B'}$ for all i, j such that $i \neq j$, we arrive at the following condition

$$|\psi_{ij}\rangle_{A''B''E} = 0 \quad s.t. \quad i \neq j \tag{2.116}$$

and thus the state that achieves the maximal violation of the CHSH inequality simplifies to

$$|\tilde{\psi}_{ABE}\rangle = |0\rangle_{A'} |0\rangle_{B'} |\psi_{00}\rangle_{A''B''E} + |1\rangle_{A'} |1\rangle_{B'} |\psi_{11}\rangle_{A''B''E}. \tag{2.117}$$

Now, we consider the other SOS relation (2.96) and plug into it the certified measurements (2.107) and (2.112). This gives us

$$\sigma_x \otimes \sigma_x \otimes \mathbb{1}_{A''B''E} |\tilde{\psi}_{ABE}\rangle = |\tilde{\psi}_{ABE}\rangle. \tag{2.118}$$

Now, substituting the simplified state (2.117), we obtain that

$$|1\rangle_{A'} |1\rangle_{B'} |\psi_{00}\rangle_{A''B''E} + |0\rangle_{A'} |0\rangle_{B'} |\psi_{11}\rangle_{A''B''E} = |0\rangle_{A'} |0\rangle_{B'} |\psi_{00}\rangle_{A''B''E} + |1\rangle_{A'} |1\rangle_{B'} |\psi_{11}\rangle_{A''B''E}. \tag{2.119}$$

Again projecting the above equation on to $\langle 0|'_A \langle 0|'_B$, we arrive at the condition that

$$|\psi_{00}\rangle_{A''B''E} = |\psi_{11}\rangle_{A''B''E}. \tag{2.120}$$

Thus, the state which achieves the maximal violation of the CHSH inequality is given by

$$U_A \otimes U_B |\psi_{ABE}\rangle = \frac{1}{\sqrt{2}} (|0\rangle_{A'} |0\rangle_{B'} + |1\rangle_{A'} |1\rangle_{B'}) \otimes |aux\rangle_{A''B''E} \tag{2.121}$$

where $|aux\rangle_{A''B''E} = \sqrt{2} |\psi_{00}\rangle_{A''B''E}$. This completes the proof that the maximal violation of CHSH Bell inequality can be used to certify the two-qubit maxmally entangled state. In Chapter 3, we generalise this proof to self-test maximally entangled state of arbitrary local dimension. We now move on to presenting the idea of one-sided device independent certification.

2.3.2 One-sided device independent certification

Let us now consider the following task inspired from a real-world scenario consisting of a bank that wants to securely send information to its clients. The security of the Bank

can be considered to be strong and chances of attack directly on the bank is much lower. However, individual clients are prone to intruders who want to steal their information. In such a situation, bank can be considered to be trusted and the clients are untrusted.

Based on the above example, let us consider a scenario where there are two parties Alice and Bob and a preparation device which sends one system to Alice and other to Bob. Here Alice is trusted, that is, she can perform a full tomography on her subsystem. Bob now performs measurements on his subsystem which might steer or affect Alice's subsystem. This scenario is in fact the quantum steering scenario. Observing some specific joint probability distribution $\{p(a,b|x,y)\}$ allows one to certify the preparation device as well the measurements performed by the untrusted Bob up to the equivalences as discussed in the previous subsection.

Definition 12 (One-sided device independent certification (1-SDI certification))**.** *Consider the above experiment with Alice and Bob performing measurements $A_{a|x}$ and $B_{b|y}$ on a state ρ_{AB} and observing correlations $\{p(a,b|x,y)\}$ along with the fact that Alice's measurements $A_{a|x}$ are known and act on Hilbert space $\mathscr{H}_A$. The state ρ_{AB} and measurements $B_{b|y}$ are certified to be the target state $|\tilde{\psi}\rangle$ and target measurements $\tilde{B}_{b|y}$ from $\{p(a,b|x,y)\}$ if:*

1. *The Hilbert space of Bob decomposes as*

$$\mathscr{H}_B = \mathscr{H}_{B'} \otimes \mathscr{H}_{B''} \tag{2.122}$$

   where the target state $|\tilde{\psi}\rangle$ belongs to $\mathscr{H}_A \otimes \mathscr{H}_{B'}$ and $\mathscr{H}_{B''}$ represents the auxiliary Hilbert space of Bob.

2. *There exists a unitary $U_B : \mathscr{H}_B \to \mathscr{H}_B$ such that the state is*

$$\left(\mathbb{1}_A \otimes U_B\right)\rho_{AB}\left(\mathbb{1} \otimes U_B^\dagger\right) = |\tilde{\psi}\rangle\langle\tilde{\psi}|_{AB'} \otimes \sigma_{B''}, \tag{2.123}$$

   where $\sigma_{B''}$ is some state acting on the Hilbert space $\mathscr{H}_{B''}$.

3. *The measurements are certified as*

$$U_B B_{b|y} U_B^\dagger = \tilde{B}_{b|y} \otimes \mathbb{1}_{B''}. \tag{2.124}$$

   where $\mathbb{1}_{B''}$ is identity acting on the Hilbert space $\mathscr{H}_{B''}$.

Analogous to self-testing, any correlation that can be used for 1SDI certification must belong to the boundary of the quantum set. As discussed before, the quantum correlations that achieve the maximal violation of a steering inequality are extremal or lie at the boundary of the quantum set. If one employs the maximum violation of a steering

inequality to certify the quantum realisations, one needs to measure much lesser number of correlations than the standard procedure of observing at least the full tomographically complete set of correlations. One can thus provide an analogous definition of 1SDI certification by replacing the line "observing correlations $\{p(a,b|x,y)\}$" by "observing the maximal violation of a steering inequality" in Def. 12. Again, we can define robust 1SDI analogously to Def. 11 imposing that Alice is trusted.

Ways to do 1SDI certification

The first results on 1SDI certification were derived in [51], [52] where the idea of swap isometry was employed to certify the maximally entangled state and Pauli observables. In [129] any pure bipartite entangled state was certified by using the subspace method as was done in [32]. There is also a numerical method [140] that aims to characterise the steering assemblages but again the limitation being that higher dimensional assemblages can not be certified in an efficient way using this method.

In chapter 4 in this thesis, we develop an analytical method for 1SDI certification. We explore the fact that the algebraic bound of the steering inequality gives some relations which can be solved to find the desired certification. Here we give a short proof to highlight this idea using the simplest steering inequality (2.61).

Let us consider the simplest steering functional (2.61) and express it in the correlation picture (2.73) as discussed above

$$W_{2,2,2} = \langle \sigma_z \otimes B_0 \rangle + \langle \sigma_x \otimes B_1 \rangle. \tag{2.125}$$

Note that for convenience, we scaled the inequality (2.61) by a factor of 2 and also removed the term corresponding to $\mathbb{1}_A \otimes \mathbb{1}_B$. Achieving the maximal quantum value implies that

$$\langle \sigma_z \otimes B_0 \rangle + \langle \sigma_x \otimes B_1 \rangle = 2. \tag{2.126}$$

Since, B_0 and B_1 are valid observables, both the terms in the above expression are upper bounded by 1. Consequently, one can achieve the quantum bound iff each of the expectation value in the above expression (2.126) is 1,

$$\sigma_z \otimes B_0 \otimes \mathbb{1}_E |\psi_{ABE}\rangle = |\psi_{ABE}\rangle \tag{2.127}$$

and,

$$\sigma_x \otimes B_1 \otimes \mathbb{1}_E |\psi_{ABE}\rangle = |\psi_{ABE}\rangle. \tag{2.128}$$

Here, as done for self-testing, we introduce an external system E to purify the state shared

between Alice and Bob. For convenience, we will drop $\mathbb{1}_E$ from further calculations. Let us recall that the measurements can be characterised only on the support of the local reduced states ρ_A and ρ_B. Thus, without loss of generality we assume that these local states are full-rank. Now multiplying (2.127) with $\sigma_x \otimes B_1$ on both the sides and then using (2.128), we arrive at

$$\sigma_x\sigma_z \otimes B_1B_0|\psi_{ABE}\rangle = \sigma_x \otimes B_1|\psi_{ABE}\rangle = |\psi_{ABE}\rangle. \tag{2.129}$$

Similarly, multiplying (2.128) with $\sigma_z \otimes B_0$ on both the sides and then using (2.127), we arrive at

$$\sigma_z\sigma_x \otimes B_0B_1|\psi_{ABE}\rangle = \sigma_z \otimes B_0|\psi_{ABE}\rangle = |\psi_{ABE}\rangle. \tag{2.130}$$

Now, using the fact that $\sigma_z\sigma_x + \sigma_x\sigma_z = 0$ in the above equation, we have that

$$\sigma_x\sigma_z \otimes B_0B_1|\psi_{ABE}\rangle = -|\psi_{ABE}\rangle. \tag{2.131}$$

Now, adding (2.129) and (2.131), we have that

$$\sigma_x\sigma_z \otimes (B_0B_1 + B_1B_0)|\psi_{ABE}\rangle = 0. \tag{2.132}$$

Since, σ_x, σ_z are invertible we get

$$\mathbb{1}_A \otimes (B_0B_1 + B_1B_0)|\psi_{ABE}\rangle = 0. \tag{2.133}$$

Now, tracing over the subsystems A, E we have

$$(B_0B_1 + B_1B_0)\rho_B = 0. \tag{2.134}$$

Again, ρ_B is full-rank and thus invertible which finally gives us the desired relation

$$B_0B_1 + B_1B_0 = 0. \tag{2.135}$$

Now, using Fact 2 we can conclude that the Hilbert space of Bob decomposes as $\mathscr{H}_B = \mathbb{C}^2 \otimes \mathscr{H}_{B''}$ and there exist a local unitary transformation $U_B : \mathscr{H}_B \to \mathscr{H}_B$ such that

$$U_BB_0U_B^\dagger = \sigma_z \otimes \mathbb{1}_{B''}, \quad \text{and} \quad U_BB_1U_B^\dagger = \sigma_x \otimes \mathbb{1}_{B''}. \tag{2.136}$$

Now, we find the state $|\psi_{ABE}\rangle$ that gives the maximum violation of the steering inequality (2.125). As was done for self-testing, we consider a general state of the form remembering

that Alice is trusted

$$\mathbb{1}_A \otimes U_B |\psi_{ABE}\rangle = |\tilde{\psi}_{ABE}\rangle = \sum_{i,j=0,1} |i\rangle_{A'} |j\rangle_{B'} |\psi_{ij}\rangle_{B''E}. \tag{2.137}$$

where $|\psi_{ij}\rangle_{B''E} \in \mathscr{H}_{B''} \otimes \mathscr{H}_E$. Now, using this state and the certified measurements (2.136), we solve the relations (2.127) and (2.128), that is,

$$\sigma_z \otimes \sigma_z \otimes \mathbb{1}_{B''} \otimes \mathbb{1}_E |\tilde{\psi}_{ABE}\rangle = |\tilde{\psi}_{ABE}\rangle \tag{2.138}$$

and,

$$\sigma_x \otimes \sigma_x \otimes \mathbb{1}_{B''} \otimes \mathbb{1}_E |\tilde{\psi}_{ABE}\rangle = |\tilde{\psi}_{ABE}\rangle. \tag{2.139}$$

Following exactly the same approach, as the one used for self-testing from Eq. (2.115) to Eq. (2.121), we find that up to a local unitary transformation U_B we have that

$$\mathbb{1}_A \otimes U_B |\psi_{ABE}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |aux\rangle_{B''E} \tag{2.140}$$

This completes our analysis of one-sided device independent certification. Now, we proceed towards another important avenue for device-independent protocols namely device-independent certification of genuine randomness.

2.3.3 Randomness certification

One of the central requirements for any cryptographic task is access to devices that can generate outputs not predictable by any attacker. Within classical framework, the security of such cryptographic tasks relies majorly on the idea that some functions can not be efficiently computed by a classical computer. For instance, the security of the RSA protocol [141] relies on the fact that large numbers can not be factored efficiently using classical computers. It was shown by Shor in 1994 [142] that one could efficiently factorise large numbers using quantum resources. Consequently, with the advent of quantum technologies, many such classical protocols have been shown to be prone to attackers possessing quantum computers. Thus, it is a matter of time when the classical cryptosystems would fail and we need better protocols that are secure against quantum attacks. This is the basis for the origin of the field of quantum cryptography.

One of the inferences that one can make about quantum theory is that it is inherently unpredictable. For instance, consider a source that generates the quantum state

$$|\psi_A\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{2.141}$$

Now, if a measurement is performed by Alice on this state in the $z-$basis, that is, $M = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, then the outcomes occur with equal probability and are unpredictable. However, here we require that the state and measurements are exactly same as the ideal ones. This is device-dependent generation of randomness, that is, one has to completely trust his devices to generate this randomness. However, let us say that the source generates the maximally entangled state

$$|\psi_{AE}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_E + |1\rangle_A|1\rangle_E) \tag{2.142}$$

instead of the state (2.141) such that some attacker Eve has access to subsystem E. Again, the measurement is performed on the subsystem A in the $z-$basis. Even if the outcomes seems unpredictable to Alice, if Eve also performs a measurement in the $z-$basis then she is able to guess the outcome of Alice with certainty as depicted in Fig. 2.7. Further, Eve might also have access to Alice's measurement device. Thus, it is necessary to find protocols for randomness generation in which one does not has to trust the device used to produce randomness. This is known as device-independent certification of randomness.

The idea of DI randomness certification schemes relies on the premise that there is some attacker who has access to the devices that are used to generate randomness. However, the attacker can only guess the outcome of the devices randomly. For instance, if the device generates two outputs, then we say that these outputs are perfectly random if chances that the attacker can guess them is never more than fifty percent. On the other hand, if the attacker can guess the outcome with certainty then the outputs are not random.

Let us now elaborate on this problem in a more formal way. Let us say that Alice performs a measurement M on a system S and observes an outcome a. Now, the attacker Eve can perform some measurement $\{Z_e\}$ on her subsystem and gets an outcome e. The outcome e is the guess that Eve makes about Alice's outcome. Then the best average probability of guessing by Eve $p_{guess}(E|S)$ has to be maximised over all possible measurements z, and thus we arrive at the following expression as suggested in Ref. [79],

$$p_{guess}(E|S) = \max_z \sum_e p(e|z)p(e=a|a,z) \tag{2.143}$$

where the above quantity $p(e=a|a,z)$ denotes the probability of Eve's outcome e to be

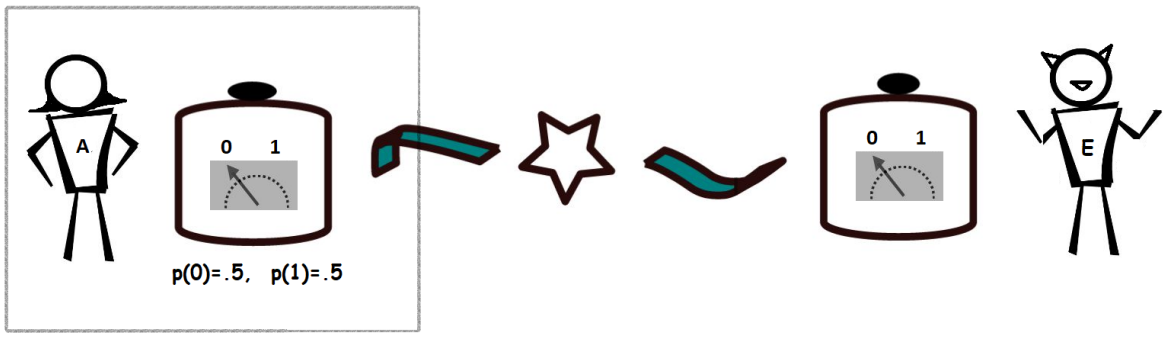


Figure 2.7: Alice locally in her lab gets perfectly random outcomes. However, her subsystem can be correlated with another subsystem possessed by an intruder Eve. Thus, locally to Alice her outcomes seem perfectly random but Eve can perfectly guess her outcome based on her results.

the same as Alice's outcome a and S denotes the system of Alice. When Alice and Eve posses quantum resources, that is, let us say that the state shared between Alice and Eve is given by ρ_{AE} and Alice performs a measurement $\{M_a\}$ and Eve performs a measurement $\{Z_e\}$ then the above guessing probability can be written as

$$p_{guess}(E|\rho_A) = \max_Z \sum_a \mathrm{Tr}(\rho_{AE} M_a \otimes Z_a) \tag{2.144}$$

where $Z = \{Z_a\}$ and $\rho_A = \mathrm{Tr}_E(\rho_{AE})$. The amount of randomness that can be generated by Alice is quantified by the min-entropy of the of the guessing probability [143], that is,

$$H_{min}(E|S) = -\log_2 p_{guess}(E|S). \tag{2.145}$$

Note that the above quantity is 0 if Eve can perfectly guess Alice's outcome. Interestingly, the maximum amount of randomness that in principle can be generated from a $d-$dimensional quantum system is of amount $2\log_2 d$ bits.

Let us now discuss how quantum non-locality, in particular, self-testing serves as a tool in designing methods for randomness certification. Consider again the Bell scenario but now with an additional party Eve (the intruder) who has access to the preparation device as well as the measurement devices of Alice and Bob. The scenario is depicted in Fig. 2.8. Now, Eve wants to guess the measurements outcome of one of the parties, let us say, Alice. In this case, Eve has the following information or strategies to guess the outcomes:

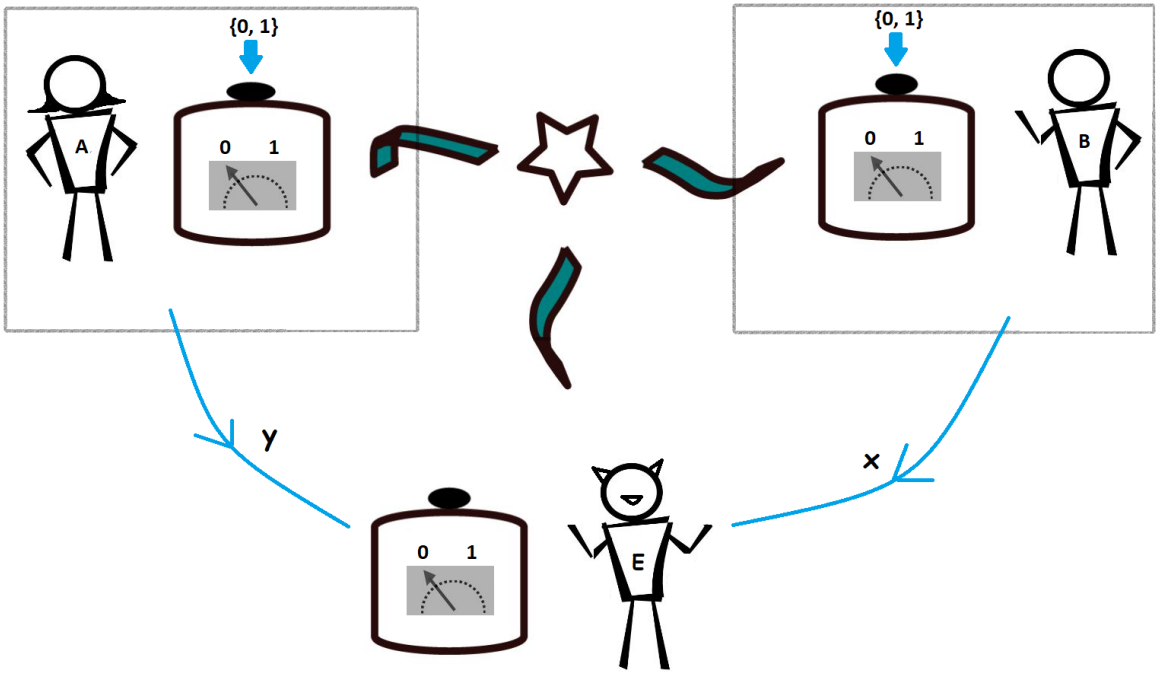


Figure 2.8: Bell scenario with an intruder Eve: In the simplest Bell scenario, we consider an additional party Eve who represents an attacker who wants to guess Alice's and Bob's outputs. She can receive some subsystem from the source correlated with the subsystem of Alice and Bob. She also might know the inputs of Alice and Bob. She uses all these information to guess their outputs by performing measurements on her received subsystem.

1. Eve can posses some subsystem E that is correlated with the state sent by the preparation device. As a consequence, the state shared among the parties is defined by $\rho_{AB} = \mathrm{Tr}_E(\rho_{ABE})$, where $\rho_{ABE} \in \mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_E$ denotes the state shared between Alice, Bob and Eve. There can not be any restriction on the dimension of the local Hilbert spaces of any of the parties. This also allows one to consider that the state shared among the parties to be pure as we can always add additional ancillary systems with Eve and purify the state.

2. Eve might have control over Alice's and Bob's measurement devices in the sense that the measurements might be performed on some auxiliary system of Alice and Bob which can interfere with their observations.

3. Eve might perform a measurement on her subsystem given by POVM $Z = \{Z_a\}$ that acts on $\mathscr{H}_E$. As discussed above, the probability of obtaining outcome a from measurement performed by Eve on her share of the joint state ρ_{ABE} is the best guess

of Alice's outcome a.

It is also necessary for Eve to remain undetected during the attack otherwise Alice and Bob can discard those runs and start over again. Thus, the joint as well as local statistics of Alice and Bob should remain equivalent to the ideal statistics as expected by them, that is,

$$\langle\psi_{ABE}|A_{a|x}\otimes B_{b|y}\otimes\mathbb{1}_E|\psi_{ABE}\rangle = \langle\tilde{\psi}_{AB}|\tilde{A}_{a|x}\otimes\tilde{B}_{b|y}|\tilde{\psi}_{AB}\rangle \tag{2.146}$$

where $|\tilde{\psi}_{AB}\rangle$ is the ideal state that is expected to be be sent by the preparation device and $\tilde{A}_{a|x}$ and $\tilde{B}_{b|y}$ represent the ideal measurement effects that are expected to be performed by the respective parties. Note that there is no constraint on Eve's measurement as Alice and Bob do not know about Eve and the statistics are averaged over Eve's outcomes. Let us denote the set of strategies as S_p that are employed by Eve such the constraint (2.146) is satisfied. Thus, the probability of Eve to guess Alice's outcome for some input x is given by,

$$G(x,P) = \sup_{S_p}\sum_a \langle\psi_{ABE}|A_{a|x}\otimes\mathbb{1}_B\otimes Z_a|\psi_{ABE}\rangle. \tag{2.147}$$

This is also known as local guessing probability [110], [144]–[146]. Here P denotes the set of observed correlations.

Now, suppose that Alice wants to generate randomness in her lab by performing the measurements A_x on the state $\rho_A = \mathrm{Tr}_{BE}(|\psi_{ABE}\rangle\langle\psi_{ABE}|)$. Now, Alice and Bob perform a Bell state using the state $|\psi_{ABE}\rangle$ and measurements A_x and B_y respectively, and observe the maximal violation of a Bell inequality. For simplicity of argument, we assume here that the measurements are projective. Let us say that the state and measurements can be self-tested from this violation to be the ideal ones, that is,

$$U_A\otimes U_B|\psi_{ABE}\rangle = |\tilde{\psi}_{A'B'}\rangle\otimes|aux\rangle_{A''B''E} \tag{2.148}$$

and the measurements on the local support of the state are certified to be the ideal measurements as

$$U_A A_x U_A^\dagger = \tilde{A}_x\otimes\mathbb{1}_{A''}, \qquad U_B B_y U_B^\dagger = \tilde{B}_y\otimes\mathbb{1}_{B''}. \tag{2.149}$$

Then the guessing probability of Eve (2.147) is given by

$$G(0,E) = \sup_{\rho_E, Z_a}\sum_a \mathrm{Tr}(\tilde{A}_{a|0}\rho_{A'})\mathrm{Tr}(Z_a\rho_E). \tag{2.150}$$

where $\rho_E = \mathrm{Tr}_{AB}(|\psi_{ABE}\rangle\langle\psi_{ABE}|)$. Using the fact $\sum_a Z_a = \mathbb{1}$, we conclude that

$$G(0,E) \leq \max_a \mathrm{Tr}(\tilde{A}_{a|0}\rho_{A'}). \tag{2.151}$$

Thus, Alice can securely generate at least

$$H_{min}(E) \geq -\log_2(\max_a \mathrm{Tr}(\tilde{A}_{a|0}\rho_{A'})) \tag{2.152}$$

amount of randomness. Notice that this bound is independent of any strategy of Eve. Thus, self-testing allows one to locally generate randomness in a highly secure way even in the presence of an intruder. This completes the subsection on randomness and the section on technical introduction. We now move onto the main results of this thesis.

Chapter 3

Certification of multipartite entangled states of arbitrary local dimension

3.1 Introduction

The strongest form of device-independent certification or self-testing has attracted considerable attention lately as it allows to obtain maximal information up to certain equivalences about a concerned quantum system with minimal assumptions. For instance, in Refs. [12]–[21], self-testing schemes have been proposed for certification of pure bipartite entangled states that are locally qubits. There are a few results that allow for certification pure bipartite entangled states of local dimension three [31], [34], [35]. A scheme for self-testing of pure bipartite states of arbitrary local dimension was proposed in [32]. However this scheme relies on self-testing of two-qubit states [12]–[14] by considering different two-dimensional subspaces of the local state of both the parties. In their scheme, one party has to perform three and the other has to perform four measurements on their respective subsystems. As far as the experimental implementation of self-testing schemes is concerned, it is thus a question of utmost importance as to whether one can design schemes exploiting the minimal number of measurements necessary to observe non-locality which is two per observer.

Self-testing schemes were also designed for multipartite states, in particular the tripartite ones, which are states shared among three parties and are locally qubits [26]–[30]. The problem to certify states shared among arbitrary number of parties has not been much explored with a few exceptions [22]–[24] that provide a scheme to self-test $N-$qubit graph states and the Dicke states. A scheme that applies to states of arbitrary local dimension and shared among arbitrary number of parties was proposed in [25]. This scheme again adapts the procedure of Ref. [32] to the multiparty scenario that relies on the self-testing

technique for the two-qubit states. Here again, one party has to perform three and the other parties have to perform four measurements. In Ref. [147], the authors show a proof-of-principle demonstration that every pure entangled state can be certified. However, in this scheme all the parties have to perform at least d^2 measurements where d is the local dimension of the state. Each of the measurements have 2^s outcomes where s is chosen such that 2^s is the smallest integer larger than d. All these limitations make this scheme practically difficult to implement in experiments.

It is thus a problem of key interest to find device-independent certification schemes that are experimentally friendly in the sense that they require minimal resources and effort for their practical implementation. We consider the general problem to design a scheme for self-testing of pure entangled states of arbitrary local dimension shared among arbitrary number of parties using Bell inequalities composed of truly $d-$outcome measurements where d is any positive integer. Further, each party must perform the minimal number of measurements possible to observe a Bell violation, which is, two.

In this Chapter, we provide a method to self-test one of most studied multipartite states, namely the N-partite Greenberger–Horne–Zeilinger (GHZ) states of local dimension d, or simply, generalised GHZ state

$$|\mathrm{GHZ}_{N,d}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes N} \tag{3.1}$$

with N and d being arbitrary integers such that $N, d \geq 2$. Notice that the generalised GHZ state (3.1) reduces to the two-qudit maximally entangled state (3.5) when $N = 2$. For this, we utilise the Bell inequalities proposed [40] which is a generalisation of the Bell inequalities proposed in [39]. In this scheme, every party needs to perform only two measurements. With the view to self-test measurements we generalise this result when each party performs arbitrary number of measurements. The results presented below are based on our works [37], [38].

3.2 Family of Bell inequalities

We consider the most general Bell scenario as depicted in Fig. 2.2. It involves N parties in spatially separated labs. Each of them receives a subsystem from a source and performs one of m $d-$outcome measurements on it. After the experiment is complete, they combine their results to reconstruct the joint probability distribution. Let us now say that we want to certify that the source generates the desired state and the parties perform the desired quantum measurements. Then, the first step to achieve this goal is to find a Bell inequality that is maximally violated by these quantum realisations. For this, we consider

two recently derived Bell inequalities.

3.2.1 SATWAP Bell inequalities

Let us first recall the Salavrakos-Augusiak-Tura-Wittek-Acín-Pironio (SATWAP) Bell inequality [39] in the simplest scenario where each party performs only two measurements. When expressed in the observable picture (cf. Chapter 2) SATWAP Bell inequality reads as

$$\mathscr{B}_{2,d,2} = \sum_{k=1}^{d-1} \left(a_k \langle A_1^k B_1^{d-k} \rangle + a_k^* \omega^k \langle A_1^k B_2^{d-k} \rangle + a_k^* \langle A_2^k B_1^{d-k} \rangle + a_k \langle A_2^k B_2^{d-k} \rangle \right) \leq \beta_C^{2,d,2}, \quad (3.2)$$

where

$$a_k = \frac{1}{\sqrt{2}} \omega^{\frac{2k-d}{8}} = \frac{1-\mathbb{i}}{2} \omega^{k/4} = \frac{1-\mathbb{i}}{2} \mathrm{e}^{\frac{\pi \mathbb{i} k}{2d}}, \quad (3.3)$$

where $\omega = e^{2\pi i/d}$ is the $d-th$ root of unity. The classical bound of the SATWAP Bell inequality $\beta_C^{2,d,2}$ was computed in [39] to be

$$\beta_C^{2,d,2} = \frac{1}{2} \left[3 \cot\left(\frac{\pi}{4d}\right) - \cot\left(3\frac{\pi}{4d}\right) \right] - 2. \quad (3.4)$$

It is worth noting that for $d = 2$ the SATWAP Bell inequality reduces to the well-known CHSH inequality (2.47) introduced in Chapter 2.

Sum of Squares (SOS) decomposition

The maximal quantum value of $\mathscr{B}_{2,2,d}$ turns out to be $\beta_Q^{2,d,2} = 2(d-1)$ and can be attained by the two-qudit maximally entangled state

$$|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle \quad (3.5)$$

and d-outcome measurements referred as Collins-Gisin-Linden-Massar-Popescu (CGLMP) measurements [148], [149]. These measurements have been experimentally realised in [150]. In the next subsection, we provide the explicit form of these measurements. As discussed in Chapter 2, to compute the quantum bound one can find the SOS decomposition of the corresponding Bell operator of SATWAP Bell inequality (3.2). To prove that $\beta_Q^{2,d,2}$ is indeed the maximum quantum value of the SATWAP Bell inequality, the following SOS decomposition was derived in [39]:

$$\beta_Q^{2,d,2} \mathbb{1} - \hat{\mathscr{B}}_{2,2,d} = \frac{1}{2} \sum_{k=1}^{d-1} \left(P_{1,k}^\dagger P_{1,k} + P_{2,k}^\dagger P_{2,k} \right), \quad (3.6)$$

with

$$P_{i,k} = \mathbb{1} - A_i^k \otimes C_i^{(k)} \tag{3.7}$$

for $i = 1,2$ and $k = 1,\ldots,d-1$ such that

$$C_1^{(k)} = a_k B_1^{-k} + a_k^* \omega^k B_2^{-k}, \qquad C_2^{(k)} = a_k^* B_1^{-k} + a_k B_2^{-k}. \tag{3.8}$$

Note from (3.3) that $a_{d-k} = a_k^*$ and thus $C_i^{(d-k)} = [C_i^{(k)}]^\dagger$ for all i,k.

3.2.2 ASTA Bell inequalities

The SATWAP Bell inequalities were later generalised to an arbitrary number of measurements per party and also to arbitrary number of parties in [40], which from here on will be referred to as Augusiak-Salavrakos-Tura-Acín (ASTA) Bell inequalities. As a matter of fact, ASTA Bell inequalities are the tilted version of Bell inequality proposed in [151]. The ASTA Bell inequalities can be expressed in the observable picture (cf. Chapter 2) as

$$\mathscr{B}_{m,d,N} := \sum_{\alpha_1,\ldots,\alpha_{N-1}=1}^{m} \sum_{k=1}^{d-1} \left\langle \left(a_k A_{1,\alpha_1}^k + a_k^* A_{1,\alpha_1+1}^k\right) \otimes \bigotimes_{i=2}^{N} A_{i,\alpha_{i-1}+\alpha_{i-1}}^{(-1)^{i-1}k} \right\rangle \geq \beta_C^{m,d,N} \tag{3.9}$$

where,

$$a_k = \frac{\omega^{\frac{2k-d}{4m}}}{2\cos(\pi/2m)}. \tag{3.10}$$

and $A_{i,x}$ is the $x-$th measurement of A_i-th party, where $\alpha_N = 1$. The classical bound of the above Bell inequality when $N = m = 2$ is given in (3.4). For some cases, such as $N = 3,4$ and $m = 2,3$ the classical bound was computed numerically in [40]. For all the other cases it is difficult to obtain the classical bound due to computational constraints. However, it was proven in [40] that the Svetlichny bound [152] of the above Bell inequalities is strictly lower than quantum bound (written below). At the same time the Svetlichny bound is known to be an upper bound to the classical bound which implies that ASTA Bell inequalities are non-trivial for any N,m,d. Recall that the Svetlichny bound is the maximal value of a Bell expression over all correlations that are convex combination of correlators that are local with respect to all possible non-trivial bipartitions.

Sum of Squares (SOS) decomposition

The maximal quantum value of $\mathscr{B}_{m,d,N}$ turns out to be $\beta_Q^{m,d,N} = m^N(d-1)$ and can be achieved by the generalised GHZ state (3.1) and the following measurements written in

the observable form as,

$$\mathscr{O}_{1,x} = U_x F_d \Omega_d F_d^\dagger U_x^\dagger, \qquad \mathscr{O}_{2,x} = V_x F_d^\dagger \Omega_d F_d V_x^\dagger, \tag{3.11}$$

for the first two parties, and for parties indexed by odd numbers as

$$\mathscr{O}_{\text{odd},x} = W_x F_d \Omega_d F_d^\dagger W_x^\dagger \tag{3.12}$$

and parties indexed by even numbers as

$$\mathscr{O}_{\text{ev},x} = W_x^\dagger F_d^\dagger \Omega_d F_d W_x \tag{3.13}$$

for all other parties A_i such that $(i = 3, \ldots, N)$. In the above formulas

$$F_d = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{ij} |i\rangle\langle j|, \qquad \Omega_d = \text{diag}[1, \omega, \ldots, \omega^{d-1}] \tag{3.14}$$

with $\omega = \exp(2\pi \mathbb{i}/d)$. Then, the unitary operations U_x, V_x and W_x are defined as

$$U_x = \sum_{j=0}^{d-1} \omega^{-j\gamma_m(x)} |j\rangle\langle j|, \qquad V_x = \sum_{j=0}^{d-1} \omega^{j\zeta_m(x)} |j\rangle\langle j|, \qquad W_x = \sum_{j=0}^{d-1} \omega^{-j\theta_m(x)} |j\rangle\langle j|, \tag{3.15}$$

where

$$\gamma_m(x) = \frac{x}{m} - \frac{1}{2m}, \qquad \zeta_m(x) = \frac{x}{m}, \qquad \text{and} \qquad \theta_m(x) = \frac{x-1}{m}. \tag{3.16}$$

The above observables can also be written in the matrix form as

$$\begin{aligned} \mathscr{O}_{1,x} &= \sum_{i=0}^{d-2} \omega^{\gamma_m(\alpha)} |i\rangle\langle i+1| + \omega^{(1-d)\gamma_m(\alpha)} |d-1\rangle\langle 0|, \\ \mathscr{O}_{2,x} &= \sum_{i=0}^{d-2} \omega^{\zeta_m(\alpha)} |i+1\rangle\langle i| + \omega^{(1-d)\zeta_m(\alpha)} |0\rangle\langle d-1| \end{aligned} \tag{3.17}$$

for the first two parties, and

$$\begin{aligned} \mathscr{O}_{\text{odd},x} &= \sum_{i=0}^{d-2} \omega^{\theta_m(\alpha)} |i\rangle\langle i+1| + \omega^{(1-d)\theta_m(\alpha)} |d-1\rangle\langle 0|, \\ \mathscr{O}_{\text{ev},x} &= \sum_{i=0}^{d-2} \omega^{\theta_m(\alpha)} |i+1\rangle\langle i| + \omega^{(1-d)\theta_m(\alpha)} |0\rangle\langle d-1| \end{aligned} \tag{3.18}$$

for the remaining parties. When $m = 2$, the measurement of the first two parties are the previously discussed CGLMP measurements. Further on, we would refer to the above measurements as generalised CGLMP measurements.

To prove that $\beta_Q^{m,d,N}$ is maximal quantum value of the ASTA Bell expression, the authors of [40] constructed the followig sum-of-squares decomposition of the Bell operator $\hat{\mathscr{B}}_{m,d,N}$,

$$\beta_Q^{m,d,N}\mathbb{1} - \hat{\mathscr{B}}_{m,d,N} = \frac{1}{2}\sum_{\alpha_1,\ldots,\alpha_{N-1}=1}^{m}\sum_{k=1}^{d-1}\left(P^{(k)}_{\alpha_1,\ldots,\alpha_{N-1}}\right)^{\dagger}P^{(k)}_{\alpha_1,\ldots,\alpha_{N-1}} + \frac{m^{N-2}}{2}\sum_{\alpha=1}^{m-2}\sum_{k=1}^{d-1}\left(R^{(k)}_{\alpha}\right)^{\dagger}R^{(k)}_{\alpha} \tag{3.19}$$

with

$$P^{(k)}_{\alpha_1,\ldots,\alpha_{N-1}} = \mathbb{1} - \overline{A}^{(k)}_{1,\alpha_1} \otimes \bigotimes_{i=2}^{N} A^{(-1)^{i-1}k}_{i,\alpha_{i-1}+\alpha_i-1} \tag{3.20}$$

and,

$$R^{(k)}_{\alpha} = \mu^*_{\alpha,k}A^k_{1,2} + \nu^*_{\alpha,k}A^k_{1,\alpha+2} + \tau_{\alpha,k}A^k_{1,\alpha+3} \tag{3.21}$$

for $k = 1,\ldots,d-1$ and all $\alpha_1,\ldots,\alpha_N$ and $\alpha = 1,2,\ldots,m-2$, where

$$\overline{A}^{(k)}_{1,\alpha_1} = a_k A^k_{1,\alpha_1} + a^*_k A^k_{1,\alpha_1+1}. \tag{3.22}$$

The coefficients $\mu_{\alpha,k}, \nu_{\alpha,k}$ and $\tau_{\alpha,k}$ are given by

$$\begin{aligned}
\mu_{\alpha,k} &= \frac{\omega^{(\alpha+1)(d-2k)/2m}}{2\cos(\pi/2m)}\frac{\sin(\pi/m)}{\sqrt{\sin(\pi\alpha/m)\sin[\pi(\alpha+1)/m]}},\\
\nu_{\alpha,k} &= -\frac{\omega^{(d-2k)/2m}}{2\cos(\pi/2m)}\frac{\sqrt{\sin[\pi(\alpha+1)/m]}}{\sqrt{\sin(\pi\alpha/m)}},\\
\tau_{\alpha,k} &= \frac{1}{2\cos(\pi/2m)}\frac{\sqrt{\sin(\pi\alpha/m)}}{\sqrt{\sin[\pi(\alpha+1)/m]}}
\end{aligned} \tag{3.23}$$

for all k and $\alpha = 1,2,\ldots,m-3$. For $\alpha = m-2$, we have

$$\begin{aligned}
\mu_{m-2,k} &= -\frac{\omega^{-k}\omega^{-(d-2k)/2m}}{2\cos(\pi/2m)\sqrt{2\cos(\pi/m)}},\\
\nu_{m-2,k} &= -\frac{\omega^{(d-2k)/2m}}{2\cos(\pi/2m)\sqrt{2\cos(\pi/m)}},\\
\tau_{m-2,k} &= \frac{\sqrt{2\cos(\pi/m)}}{2\cos(\pi/2m)}.
\end{aligned} \tag{3.24}$$

Note from (3.3) that $a_{d-k} = a^*_k$ and thus $\overline{A}^{(d-k)}_i = [\overline{A}^{(k)}_i]^{\dagger}$ for all i,k. For our considerations, we also construct several analogous sum-of-squares decomposition parametrized of the Bell

operator $\hat{\mathscr{B}}_{m,d,N}$ given by

$$\beta_Q \mathbb{1} - \hat{\mathscr{B}}_{N,m,d} = \frac{1}{2} \sum_{\alpha_1,\ldots\alpha_N=1,2} \sum_{k=1}^{d-1} P^{(k)}_{n,\alpha_1,\ldots\alpha_N} P^{(k)\dagger}_{n,\alpha_1,\ldots\alpha_N} + \frac{m^{N-2}}{2} \sum_{\alpha=1}^{m-2} \sum_{k=1}^{d-1} \left(R^{(k)}_{n,\alpha}\right)^{\dagger} R^{(k)}_{n,\alpha}, \quad (3.25)$$

where $n = 2,3,\ldots,N$. In the above decomposition (3.25), we have that

$$P^{(k)}_{n,\alpha_1,\ldots,\alpha_N} = \mathbb{1} - A^{(k)}_{1,\alpha_1} \otimes \overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1} \otimes \bigotimes_{\substack{i=2 \\ i\neq n}}^{N} A^{(-1)^{i-1}k}_{i,\alpha_{i-1}+\alpha_i-1}. \quad (3.26)$$

For odd n, $\overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1}$ and $R^{(k)}_{n,\alpha}$ are defined as

$$\overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1} = a_k A^{k}_{n,\alpha_{n-1}+\alpha_n-1} + a^*_k A^{k}_{n,\alpha_{n-1}+\alpha_n} \quad (3.27)$$

and,

$$R^{(k)}_{n,\alpha} = \mu^*_{\alpha,k} A^k_{n,2} + \nu^*_{\alpha,k} A^k_{n,\alpha+2} + \tau_{\alpha,k} A^k_{n,\alpha+3}, \quad (3.28)$$

whereas, if n is even then

$$\overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1} = a_k A^{-k}_{n,\alpha_{n-1}+\alpha_n-1} + a^*_k A^{-k}_{n,\alpha_{n-1}+\alpha_n-2} \quad (3.29)$$

and,

$$R^{(k)}_{n,\alpha} = \mu_{\alpha,k} A^{-k}_{n,2} + \nu_{\alpha,k} A^{-k}_{n,\alpha+2} + \tau_{\alpha,k} A^{-k}_{n,\alpha+3}. \quad (3.30)$$

It is important to note here that $A_{n,\alpha+m} = \omega A_{n,\alpha}$ and $A_{n,0} = \omega^{-1} A_{n,m}$ for all n, α. Further, the coefficients $\mu_{\alpha,k}$, $\nu_{\alpha,k}$ and $\tau_{\alpha,k}$ appearing in conditions (3.28) and (3.30) are given in Eq. (3.23) and Eq. (3.24).

Before moving on to the proof of self-testing, let us introduce the following unitary matrices which are essential for our considerations. The first matrix is the $d-$dimensional generalisation of the Pauli-z matrix

$$Z_d = \sum_{i=0}^{d-1} \omega^i |i\rangle\langle i| \quad (3.31)$$

and second,

$$T_{d,m} = \sum_{i=0}^{d-1} \omega^{i+\frac{1}{m}} |i\rangle\langle i| - \frac{2\mathbb{i}}{d} \sin\left(\frac{\pi}{m}\right) \sum_{i,j=0}^{d-1} (-1)^{\delta_{i,0}+\delta_{j,0}} \omega^{\frac{i+j}{2}-\frac{d-2}{2m}} |i\rangle\langle j|. \tag{3.32}$$

Notice that the above matrices represent valid observabales, that is, they are unitaries with eigenvalues $1, \omega, \ldots, \omega^{d-1}$. Also notice that when $d = m = 2$, the second matrix is proportional to Pauli-x matrix, that is, $T_{2,2} = -\sigma_x$.

3.3 Self-testing

Here, we demonstrate how achieving the maximal value of the ASTA Bell inequalities (3.9), that is, $\mathscr{B}_{m,d,N} = \beta_Q$, can be used for self-testing of generalised GHZ states (3.1) and the generalised CGLMP measurements (3.11),(3.12) and (3.13). Let us first recall that we can only characterise the observables on the support of the local states ρ_{A_i}. Thus, without loss of generality we can assume them to be of full rank. The main result comprises of one long proof and is very technical. To make it easier to follow, we shift some parts of the proof to Appendix and refer them here as Lemmas.

Theorem 3.1. *Assume that all the parties A_i perform the Bell experiment and observe that the Bell inequality (3.9) is maximally violated, that is, $\beta_Q^{m,d,N} = m^N(d-1)$ where N is number of parties, d denotes the number of outcomes of each measurement and m is the number of measurements performed by each party. Let us now say that the maximal quantum bound is achieved using the state ρ_N acting on $\mathscr{H}_{A_1} \otimes \ldots \otimes \mathscr{H}_{A_N}$ and unitary observables $A_{i,\alpha}$ for all i and $\alpha \in \{1,2,\ldots,m\}$ acting on $\mathscr{H}_{A_i}$. Then, the following statements hold true:*

1. *The Hilbert space $\mathscr{H}_{A_i}$ of all the parties A_i admits a decomposition into a $d-$dimensional Hilbert space $\mathbb{C}^d$ and an auxiliary Hilbert space of unkown but finite dimension $\mathscr{H}_{A_i''}$,*

$$\mathscr{H}_{A_i} = (\mathbb{C}^d)_{A_i'} \otimes \mathscr{H}_{A_i''}. \tag{3.33}$$

2. *A local unitary transformation $U_{A_i} : \mathscr{H}_{A_i} \to \mathscr{H}_{A_i}$ can be applied on each side, such that*

$$(U_1 \otimes \ldots \otimes U_N)\, \rho_N \left(U_1^\dagger \otimes \ldots \otimes U_N^\dagger\right) = |\mathrm{GHZ}_{N,d}\rangle\langle \mathrm{GHZ}_{N,d}|_{A_1'A_2'\ldots A_N'} \otimes \rho^{\mathrm{aux}}_{A_1''A_2''\ldots A_N''} \tag{3.34}$$

where $|\mathrm{GHZ}_{N,d}\rangle$ is the generalised GHZ state (3.1) and

$$\forall i, \alpha, \qquad U_i A_{i,\alpha} U_i^\dagger = \mathscr{O}_{i,\alpha} \otimes \mathbb{1}_i'' \tag{3.35}$$

where A_i'' denotes the auxiliary system of every party on which the measurements act trivially and $\mathbb{1}_i''$ acts on the Hilbert space $\mathscr{H}_{A_i''}$.

Proof. The proof consists of two major steps. The first one is divided into two sub-steps. In the first of them, we concentrate on the first party and prove that in $\mathscr{H}_{A_1}$ one can identify a qudit in the sense of Eq. (3.33). Then, the observables $A_{1,x}$ can be certified up to local unitary to be the generalised CGLMP measurement (3.11). In the next sub-step, we extend the above proofs to the remaining parties. For our convinience, in the proof we consider a purification of the state ρ_N by adding an ancillary system E and $|\psi_N\rangle \in \mathscr{H}_1 \otimes \ldots \otimes \mathscr{H}_N \otimes \mathscr{H}_E$ such that $\rho_N = \mathrm{Tr}_E(|\psi\rangle\langle\psi|_N)$.

In the second major step of the proof, we use the obtained observables to certify that $|\psi_N\rangle$ is unitarily equivalent to the generalised GHZ state (3.1).

The Hilbert space structure and characterization of observables

The first party

To begin, as discussed in Chapter 2, we notice that any state $|\psi\rangle_N \in \mathscr{H}_{A_1} \otimes \ldots \otimes \mathscr{H}_{A_N} \otimes \mathscr{H}_E$ that maximally violates the Bell inequalities (3.9) must satisfy the following relation due to the SOS decomposition (3.19),

$$P^{(k)}_{\alpha_1,\ldots,\alpha_N} \otimes \mathbb{1}_E |\psi_N\rangle = 0 \tag{3.36}$$

for $k = 1,2,\ldots,d-1$ and $\alpha_i = 1,2,\ldots,m$ for $i = 1,2,\ldots,N-1$ and $\alpha_N = 1$. Expanding the above term with the aid of Eq. (3.20), this implies that

$$\overline{A}^{(k)}_{1,\alpha_1} \otimes \bigotimes_{i=2}^{N} A^{(-1)^{i-1}k}_{i,\alpha_{i-1}+\alpha_i-1} \otimes \mathbb{1}_E |\psi_N\rangle = |\psi_N\rangle \tag{3.37}$$

for all k and α_i. From here on, for simplicity we drop the term $\mathbb{1}_E$. Since A_{i,α_i} are unitary for all i and α_i, we have that

$$\overline{A}^{(k)}_{1,\alpha_1} \otimes \mathbb{1}_{A_2A_3\ldots A_N} |\psi_N\rangle = \mathbb{1}_{A_1} \otimes \bigotimes_{i=2}^{N} A^{(-1)^{i}k}_{i,\alpha_{i-1}+\alpha_i-1} |\psi_N\rangle. \tag{3.38}$$

After applying $\mathbb{1}_{A_1} \otimes \bigotimes_{i=2}^{N} A^{(-1)^{i-1}k}_{i,\alpha_{i-1}+\alpha_i-1}$ to the above condition and taking into account Eq. (3.38) for $k \to d-k$, we arrive at

$$\overline{A}^{(k)}_{1,\alpha_1} \overline{A}^{(d-k)}_{1,\alpha_1} \otimes \mathbb{1}_{A_2A_3\ldots A_N} |\psi_N\rangle = |\psi_N\rangle. \tag{3.39}$$

Taking then the partial trace over the subsystems $A_2, A_3, \ldots, A_N, E$ we obtain

$$\overline{A}^{(k)}_{1,\alpha_1} \overline{A}^{(d-k)}_{1,\alpha_1} \rho_{A_1} = \rho_{A_1}, \tag{3.40}$$

where $\rho_{A_1} = \mathrm{Tr}_{A_2,A_3,\ldots,A_N,E}(|\psi\rangle\langle\psi|_N)$. Since, ρ_{A_1} is full-rank and thus invertible, we conclude from the above formula that

$$\overline{A}^{(k)}_{1,\alpha_1} \overline{A}^{(d-k)}_{1,\alpha_1} = \mathbb{1}. \tag{3.41}$$

Now, using the relation (3.38) for $k = 1$, and then applying $\overline{A}^{(1)}_{1,\alpha_1}$ recursively to it, we also obtain that

$$\overline{A}^{(k)}_{1,\alpha_1} = \left[\overline{A}^{(1)}_{1,\alpha_1}\right]^k \tag{3.42}$$

for all k, α_1. Recall that $\overline{A}^{(d-k)}_{1,\alpha_1} = \overline{A}^{(k)\dagger}_{1,\alpha_1}$ for any $k = 1, \ldots, d-1$. The other term in the SOS decomposition (3.19) yields the following relation,

$$R^{(k)}_\alpha |\psi_N\rangle = 0 \qquad \forall k, \alpha. \tag{3.43}$$

Note that $R^{(k)}_\alpha$ is composed of only $A'_1 s$ observables and thus acts only on the first party's subsystem ρ_{A_1}. Taking a partial trace over the subsystems $A_2, A_3, \ldots, A_N, E$, the above condition is equivalent to $R^{(k)}_\alpha \rho_{A_1} = 0$. Again, taking into account that ρ_{A_1} is full-rank and thus inevertible, we have that

$$R^{(k)}_\alpha = 0 \tag{3.44}$$

for all k and α. The conditions (3.41), (3.42) and (3.44) are solely composed of the $A'_1 s$ observables and as a matter of fact, enough to characterise the observables A_{1,α_1} for all α_1 up to local unitary operations.

From here on, for simplicity we denote $\mathscr{H}_{A_1}$ as $\mathscr{H}_1$ and $\mathscr{H}_{A'_1}$ as $\mathscr{H}''_1$. Let us first give short overview of the idea behind the proof. First, we show that the Hilbert space of first party can be written as a direct sum of $d-$dimensional Hilbert space, that is,

$$\mathscr{H}_1 = \mathbb{C}^d \otimes \mathscr{H}''_1, \tag{3.45}$$

where $\mathscr{H}''_1$ is a Hilbert of unknown but finite dimension. For this purpose, using the conditions (3.41) and (3.42) for $\alpha_1 = 2$, we show in Lemma 3.1 which is stated below that

$$\mathrm{Tr}(A^n_{1,2}) = \mathrm{Tr}(A^n_{1,3}) = 0 \tag{3.46}$$

for any n that is a divisor of d such that $n < d$. Then using (3.44), we can also conclude

the same result for the rest of the observbales, that is, $\mathrm{Tr}(A_{1,\alpha}^n) = 0$ for all $\alpha = 1,2,\ldots,m$ and any n that is a divisor of d such that $n < d$. Notice that for a unitary matrix M with eigenvalues m_i, we have that $\mathrm{Tr}(M^n) = \sum_{i=0}^{d-1} m_i^n$ for any n. Thus from (3.46), we can conclude that

$$\mathrm{Tr}(A_{1,2}^n) = \sum_i \lambda_i \omega^{in} = 0 \tag{3.47}$$

for any n that is a divisor of d, where λ_i is the multiplicity of the eigenvalue ω^i. Now using Fact 3 stated below, whose proof can be found in [37], we can conclude that the multiplicities of these eigenvalues are equal, that is, $\lambda_0 = \lambda_1 = \ldots = \lambda_{d-1}$.

Fact 3. *Consider a real polynomial*

$$W(x) = \sum_{i=0}^{d-1} \lambda_i x^i \tag{3.48}$$

with rational coefficients $\lambda_i \in \mathbb{Q}$. Assume that ω^n with $\omega = \mathrm{e}^{2\pi \mathrm{i}/d}$ is a root of $W(x)$ for any n being a proper divisor of d, i.e., $n \neq d$ such that $d/n \in \mathbb{N}$. Then, $\lambda_0 = \lambda_1 = \ldots = \lambda_{d-1}$.

This allows us to conclude that the observables of A_1 act on a Hilbert space $\mathscr{H}_1$ of dimension $d \times D$ where D is positive integer. Moreover, one can always rotate one of $A_1's$ observables to some observable that acts on $\mathbb{C}^d$ tensored with identity acting on $\mathscr{H}_1''$ (3.45). Precisely one can find a unitary transformation $V_1 : \mathscr{H}_1 \to \mathscr{H}_1$ such that

$$V_1 A_{1,2} V_1^\dagger = Z_d \otimes \mathbb{1}_1'', \tag{3.49}$$

where Z_d is defined in Eq. (3.32). Then in Lemma 3.2, using the above form of $A_{1,2}$, we show that $A_{1,3}$ is also unitarily equivalent to an observable acting on a $\mathbb{C}^d$ tensored with identity acting on $\mathscr{H}_1''$, that is,

$$V_1 A_{1,3} V_1^\dagger = T_{d,m} \otimes \mathbb{1}_1'' \tag{3.50}$$

with $T_{d,m}$ defined in Eq. (3.32). Next, we find a unitary transformation $U_1 : \mathscr{H}_1 \to \mathscr{H}_1$ stated in Fact 3.3 of Appendix B, that rotate these observables to the ideal ones, that is,

$$U_1 A_{1,\alpha_1} U_1^\dagger = \mathscr{O}_{1,\alpha_1} \otimes \mathbb{1}_1'' \quad \text{for} \quad \alpha_1 = 2,3. \tag{3.51}$$

Finally, using the derived observables and the condition (3.44) we find the rest of the observables A_{1,α_1}. For this, we first consider the relation (3.44) for $k = 1$ and $\alpha = 1$. After

plugging the explicit form of $R_1^{(1)}$ from (3.21) we have that

$$\mu^*_{1,1}A_{1,2} + \nu^*_{1,1}A_{1,3} + \tau_{1,1}A_{1,4} = 0. \tag{3.52}$$

Plugging the observables $A_{1,2}$ and $A_{1,3}$ from (3.51), we find that

$$U_1 A_{1,4} U_1^\dagger = \mathscr{O}_{1,4} \otimes \mathbb{1}''_1. \tag{3.53}$$

The above statement is easy to conclude based on the fact that the ideal observables satisfy the condition (3.44) derived from the maximal violation of the Bell inequalities. Continuing this procedure recursively for the remaining values of α_1, we see that

$$U_1 A_{1,\alpha_1} U_1^\dagger = \mathscr{O}_{1,\alpha_1} \otimes \mathbb{1}''_1 \qquad \forall \alpha_1. \tag{3.54}$$

Now let us prove the two lemmas which were used to arrive at the desired form of the observables (3.54).

Lemma 3.1. *Consider two unitary observables $A_{1,2}$ and $A_{1,3}$ with eigenvalues $\{1, \omega, \ldots, \omega^{d-1}\}$ that act on a finite-dimensional Hilbert space and satisfy the conditions (3.41) and (3.42). Then for any n that is a divisor of d such that $n < d$ we have that,*

$$\mathrm{Tr}(A^n_{1,2}) = 0, \quad \textit{and} \qquad \mathrm{Tr}(A^n_{1,3}) = 0. \tag{3.55}$$

Proof. To begin the proof, let us consider the relations (3.41) for $\alpha_1 = 2$, in which we substitute the explicit form of $\overline{A}_{1,2}$ (3.22),

$$\left(a_k A^k_{1,2} + a^*_k A^k_{1,3}\right)\left(a^*_k A^{-k}_{1,2} + a_k A^{-k}_{1,3}\right) = \mathbb{1}. \tag{3.56}$$

Simplifying the above expression and then plugging in the value of a_k from (3.10) leads us to the following condition,

$$\omega^{\frac{2k-d}{2m}} A^k_{1,2}A^{-k}_{1,3} + \omega^{-\frac{2k-d}{2m}} A^k_{1,3}A^{-k}_{1,2} = 2\cos\left(\frac{\pi}{m}\right)\mathbb{1}. \tag{3.57}$$

We multiply the above equation (3.57) by $A^k_{1,3}$ and then take the trace to obtain

$$\omega^{\frac{2k-d}{2m}} \mathrm{Tr}(A^k_{1,2}) + \omega^{-\frac{2k-d}{2m}} \mathrm{Tr}(A^{2k}_{1,3}A^{-k}_{1,2}) = 2\cos\left(\frac{\pi}{m}\right)\mathrm{Tr}(A^k_{1,3}). \tag{3.58}$$

Let us again consider the second relation (3.42) for $\alpha_1 = 2$ where we substitute $\overline{A}_{1,2}$ and

a_k from (3.22) and (3.10) respectively, to obtain,

$$a_{2k}A_{1,2}^{2k} + a_{2k}^* A_{1,3}^{2k} = \left(a_k A_{1,2}^k + a_k^* A_{1,3}^k\right)\left(a_k A_{1,2}^k + a_k^* A_{1,3}^k\right) \tag{3.59}$$

for $k = 1, \ldots, \lfloor \frac{d}{2} \rfloor$ where $\lfloor x \rfloor$ is the largest integer smaller than x. A simple calculation using the explicit form of a_k and some trigonometric identities leads us to

$$\omega^{k/m} A_{1,2}^{2k} + \omega^{-k/m} A_{1,3}^{2k} = A_{1,2}^k A_{1,3}^k + A_{1,3}^k A_{1,2}^k. \tag{3.60}$$

We then multiply the above equation (3.60) by $A_{1,2}^{-k}$ and take the trace to get

$$\omega^{k/m}\mathrm{Tr}(A_{1,2}^k) + \omega^{-k/m}\mathrm{Tr}(A_{1,3}^{2k}A_{1,2}^{-k}) = 2\mathrm{Tr}(A_{1,3}^k). \tag{3.61}$$

After substituting the term $\mathrm{Tr}(A_{1,3}^{2k}A_{1,2}^{-k})$ from (3.61) to the above equation (3.58), we obtain that

$$\mathrm{Tr}(A_{1,2}^k) = 2\omega^{-k/m}\frac{1-\cos(\pi/m)\omega^{-d/2m}}{1-\omega^{-d/m}}\mathrm{Tr}(A_{1,3}^k). \tag{3.62}$$

Using the fact that

$$\cos\left(\frac{\pi}{m}\right) = \frac{1}{2}\left(\omega^{-\frac{d}{2m}} + \omega^{\frac{d}{2m}}\right), \tag{3.63}$$

we can simplify the relation (3.62) to the following form

$$\mathrm{Tr}(A_{1,2}^k) = \omega^{-k/m}\mathrm{Tr}(A_{1,3}^k) \qquad k = 1, \ldots, \left\lfloor \frac{d}{2} \right\rfloor. \tag{3.64}$$

To prove that the traces of these observables vanish, we use the following observation whose proof is deferred to Appendix B.

Observation 3.1. *Consider two unitary observables $A_{1,2}$ and $A_{1,3}$ with eigenvalues $\{1, \omega, \ldots, \omega^{d-1}\}$ that act on a finite-dimensional Hilbert space and satisfy the conditions (3.41) and (3.42). Then for any n that is a divisor of d such that $n < d$ we have that,*

$$\mathrm{Tr}(A_{1,2}^x) = \omega^{\frac{2tx}{m}}\,\mathrm{Tr}\left(A_{1,2}^{(2t+1)x}A_{1,3}^{-2tx}\right). \tag{3.65}$$

for any non-negative integer $t \in \mathbb{N} \cup \{0\}$ and $x = 1, \ldots, \lfloor d/2 \rfloor$

Now, consider a positive integer n that is a divisor of d, that is, $d/n \in \mathbb{N}$ where $\mathbb{N}$ denotes the set of natural numbers[1]. Now, d/n can be either even or odd. Let us first

[1] As a matter of fact, any non-trivial divisor of d is always less than or equal to $d/2$.

consider the case, when d/n is even. This implies that there is an integer t such that $2t = d/n$. Substituting $x = n = d/2t$ in the conditon (3.65) we obtain that

$$\mathrm{Tr}(A_{1,2}^n) = \omega^{d/m}\,\mathrm{Tr}(A_{1,2}^{d+n}A_{1,3}^{-d}). \tag{3.66}$$

The above relation can be simplified to

$$\mathrm{Tr}(A_{1,2}^n) = \omega^{d/m}\mathrm{Tr}(A_{1,2}^n). \tag{3.67}$$

where we used the fact that $A_{1,2}^d = A_{1,3}^{-d} = \mathbb{1}$. Thus, for any $m \geq 2$, the only possible solution of the above condition is $\mathrm{Tr}(A_{1,2}^n) = 0$ for any n such that d/n is even. Using then Eq. (3.64) one can similarly conclude that $\mathrm{Tr}(A_{1,3}^n) = 0$. Now, consider the second case, that is, n is a divisor of d such that d/n is odd. This implies that there is an integer t such that $2t+1 = d/n$. Substituting $x = n = d/(2t+1)$ again in condition (3.65), we obtain that

$$\mathrm{Tr}(A_{1,2}^n) = \omega^{d/m}\omega^{-n/m}\,\mathrm{Tr}\left(A_{1,3}^n\right). \tag{3.68}$$

Comparing the above expression with Eq. (3.64), one directly concludes that $\mathrm{Tr}(A_{1,\alpha}) = 0$ for any n such that d/n is odd and $n \leq d/2$. Thus, we have shown that for any n which is a divisor of d, $\mathrm{Tr}(A_{1,\alpha}^n) = 0$ for $\alpha = 2,3$. This completes the proof of Lemma 3.1. □

Now, we move onto finding the explicit form of the measurements $A_{1,\alpha}$ for $\alpha = 2,3$.

Lemma 3.2. *Consider two unitary observables $A_{1,2}$ and $A_{1,3}$ with eigenvalues $\{1,\omega,\ldots,\omega^{d-1}\}$ that act on a $\mathbb{C}^d \otimes \mathscr{H}_1''$ such that $\mathscr{H}_1''$ is a finite-dimensional Hilbert space and satisfy the conditions (3.41) and (3.42). Then, we can find a unitary $V_1 : \mathscr{H}_1 \to \mathscr{H}_1$ that transforms $A_{1,2}$ and $A_{1,3}$ as*

$$V_1 A_{1,2} V_1^\dagger = Z_d \otimes \mathbb{1}_1'' \tag{3.69}$$

and

$$V_1 A_{1,3} V_1^\dagger = T_{d,m} \otimes \mathbb{1}_1'' \tag{3.70}$$

where $Z_d, T_{d,m}$ are defined in (3.31) and (3.32).

Proof. Let us begin by proving a relation between $A_{1,2}$ and $A_{1,3}$ given by,

$$A_{1,3}^k = -(k-1)\omega^{\frac{k}{m}}A_{1,2}^k + \omega^{\frac{k-1}{m}}\sum_{t=0}^{k-1} A_{1,2}^t A_{1,3} A_{1,2}^{k-1-t}. \tag{3.71}$$

for any $k = 1,\ldots,d$. To prove the above relation, we use the technique of mathematical

induction. We can easily check that this relation (3.71) holds trivially for $k=1$. Now, let us assume that this relation (3.71) holds for some $k=s$. To prove that it also holds for $k=s+1$, we need to examine (3.42) for $\alpha_1=2$ and $k=s+1$

$$\overline{A}_{1,2}^{(s+1)} = \left[\overline{A}_{1,2}^{(1)}\right]^{(s)} \overline{A}_{1,2}^{(1)}. \tag{3.72}$$

for $s=1,\ldots,d-1$. Again, using (3.42) for $\alpha_1=2$ and $k=s$ on the right hand side of the above equation, we have that

$$\overline{A}_{1,2}^{(s+1)} = \overline{A}_{1,2}^{(s)}\overline{A}_{1,2}^{(1)}. \tag{3.73}$$

Expanding $\overline{A}_{1,2}^{(s)}$ using (3.22) and then simplifying the obtained expression with the aid of the formula $a_{s+1}-a_s a_1 = \omega^{\frac{s+1}{2m}}/2\cos^2(\pi/2m)$, we obtain that

$$A_{1,3}^{s+1} = -\omega^{\frac{s+1}{m}} A_{1,2}^{s+1} + \omega^{\frac{s}{m}} A_{1,2}^{s} A_{1,3} + \omega^{\frac{1}{m}} A_{1,3}^{s} A_{1,2}. \tag{3.74}$$

Replacing $A_{1,3}^{s}$ using the relation (3.71) into the above equation, we arrive at

$$A_{1,3}^{s+1} = -\omega^{\frac{s+1}{m}} A_{1,2}^{s+1} + \omega^{\frac{s}{m}} A_{1,2}^{s} A_{1,3} + \omega^{\frac{1}{m}} \left[-(s-1)\omega^{\frac{s}{m}} A_{1,2}^{s} + \omega^{\frac{s-1}{m}} \sum_{t=0}^{s-1} A_{1,2}^{t} A_{1,3} A_{1,2}^{s-1-t}\right] A_{1,2} \tag{3.75}$$

which on simplification gives us the above relation (3.71) for $k=s+1$,

$$A_{1,3}^{s+1} = -s\omega^{\frac{s+1}{m}} A_{1,2}^{s+1} + \omega^{\frac{s}{m}} \sum_{t=0}^{s} A_{1,2}^{t} A_{1,3} A_{1,2}^{s-t}. \tag{3.76}$$

As discussed before, $A_{1,2}$ and $A_{1,3}$ act on $\mathbb{C}^d \otimes \mathscr{H}_1''$ and therefore we can always find a a unitary $\overline{V}_1 : \mathscr{H}_1 \to \mathscr{H}_1$ such that $\overline{V}_1 A_{1,2} \overline{V}_1^{\dagger} = Z_d \otimes \mathbb{1}_1''$. Let us then decompose $A_{1,3}$ under the action of $\overline{V}_1$ as

$$\overline{V}_1 A_{1,3} \overline{V}_1^{\dagger} = \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes F_{ij}, \tag{3.77}$$

where F_{ij} for $i,j=0,1,\ldots,d-1$ are matrices acting on $\mathscr{H}_1''$. Notice that any matrix acting on a Hilbert space $\mathbb{C}^d \otimes \mathscr{H}_1''$ can be decomposed in this way. From here on, for simplicity we drop the unitary V_1 and recall it back at the end of the proof of this lemma. Also, we simplify the notation by replacing $\mathbb{1}_1''$ by $\mathbb{1}$ and use the correct notation at the end of the proof.

For characterising $A_{1,3}$, it is now enough to find the matrices F_{ij}. To do this we first determine the matrices F_{ii} for all i using the relations (3.71). Using then the derived F_{ii}, we then proceed to determine F_{ij} for $i \neq j$. Let us now consider the relation (3.71) for

$k = d-1$,

$$A_{1,3}^{\dagger} = -(d-2)\omega^{\frac{d-1}{m}} A_{1,2}^{\dagger} + \omega^{\frac{d-2}{m}} \sum_{t=0}^{d-2} A_{1,2}^{t} A_{1,3} A_{1,2}^{d-t-2}. \tag{3.78}$$

Substituting $A_{1,2} = Z_d \otimes \mathbb{1}$ and $A_{1,3}$ from (3.77) in the above expression (3.78) and then simplifying it, we arrive at

$$\sum_{i,j=0}^{d-1} |j\rangle\langle i| \otimes F_{ij}^{\dagger} = -(d-2)\omega^{\frac{d-1}{m}} \sum_{i=0}^{d-1} \omega^{-i} |i\rangle\langle i| \otimes \mathbb{1} + \omega^{\frac{d-2}{m}} \sum_{i,j=0}^{d-1} \sum_{t=0}^{d-2} \omega^{-2j+t(i-j)} |i\rangle\langle j| \otimes F_{ij}. \tag{3.79}$$

Sandwiching the above equation with $\langle i|.|i\rangle$, we get the following expression

$$F_{ii}^{\dagger} = -(d-2)\omega^{\frac{d-1}{m}} \omega^{-i} \mathbb{1} + (d-1)\omega^{\frac{d-2}{m}} \omega^{-2i} F_{ii}. \tag{3.80}$$

We can get another relation by its Hermitian conjugation,

$$F_{ii} = -(d-2)\omega^{-\frac{d-1}{m}} \omega^{i}\, \mathbb{1} + (d-1)\omega^{-\frac{d-2}{m}} \omega^{2i} F_{ii}^{\dagger}. \tag{3.81}$$

Substituting $F_{ii}^{\dagger}$ from the first relation (3.80) into the above formula (3.81) we arrive at

$$F_{ii} = -(d-2)\omega^{-\frac{d-1}{m}} \omega^{i}\, \mathbb{1} - (d-2)(d-1)\omega^{\frac{1}{m}+i} \mathbb{1} + (d-1)^2 F_{ii}, \tag{3.82}$$

which after rearranging the terms simplifies to,

$$F_{ii} = \omega^{i+\frac{1}{m}} \left(\frac{d-1+\omega^{-\frac{d}{m}}}{d} \right) \mathbb{1} = \omega^{i+\frac{1}{m}} \left(1 - \frac{2\mathbb{i} \sin(\pi/m)}{d} \omega^{-\frac{d}{2m}} \right) \mathbb{1}. \tag{3.83}$$

where we used the trigonometric identity

$$\sin\left(\frac{\pi}{m}\right) = \frac{1}{2\mathbb{i}} \left(\omega^{\frac{d}{2m}} - \omega^{\frac{d}{2m}} \right). \tag{3.84}$$

After determining F_{ii} we proceed towards finding the matrices F_{ij} for $i \neq j$. The first observation can be simply made by considering the relation (3.79) and sandwiching it with $\langle i|.|j\rangle$ for $i \neq j$, to get

$$F_{ji}^{\dagger} = \omega^{\frac{d-2}{m}} \omega^{-2j} \sum_{t=0}^{d-2} \omega^{t(i-j)} F_{ij}. \tag{3.85}$$

Using the fact that $\sum_{t=0}^{d-2} \omega^{t(i-j)} = -\omega^{-(i-j)}$ for $i \neq j$, the above equation reduces to

$$F_{ij} = -\omega^{-\frac{d-2}{m}} \omega^{i+j} F_{ji}^{\dagger}. \tag{3.86}$$

Finding the exact form of F_{ij} requires another observation that involves higher order terms in F_{ij}. Due to highly technical nature of the proof, we defer it to Appendix B.

Observation 3.2. *The following conditions hold true for any $k = 1, \ldots, d-1$ and $m \geq 2$,*

$$\begin{aligned} -(k-1) \sum_{i,j=0}^{d-1} \omega^{ki} |i\rangle\langle j| \otimes F_{ij} + \omega^{-\frac{1}{m}} \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes \left[\sum_{\substack{l=0 \\ l\neq i}}^{d-1} \left(\frac{\omega^{ki} - \omega^{kl}}{\omega^i - \omega^l} \right) F_{il} F_{lj} + k\omega^{(k-1)i} F_{ii} F_{ij} \right] \\ = -k\omega^{\frac{1}{m}} \sum_{i=0}^{d-1} \omega^{(k+1)i} |i\rangle\langle i| \otimes \mathbb{1} + \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes \sum_{t=0}^{k} \omega^{kj+t(i-j)} F_{ij}. \end{aligned} \tag{3.87}$$

We sandwich the relation (3.87) with $\langle i|.|i\rangle$ to get

$$\begin{aligned} -(k-1) \sum_{i=0}^{d-1} \omega^{ki} F_{ii} + \omega^{-\frac{1}{m}} \sum_{i=0}^{d-1} \left[\sum_{\substack{l=0 \\ l\neq i}}^{d-1} \left(\frac{\omega^{ki} - \omega^{kl}}{\omega^i - \omega^l} \right) F_{il} F_{li} + k\omega^{(k-1)i} F_{ii}^2 \right] \\ = -k\omega^{\frac{1}{m}} \sum_{i=0}^{d-1} \omega^{(k+1)i} \mathbb{1} + \sum_{i=0}^{d-1} \sum_{t=0}^{k} \omega^{ki} F_{ii} \end{aligned} \tag{3.88}$$

which after some simple rearrangement of the terms gives us

$$\sum_{\substack{l=0 \\ l\neq i}}^{d-1} \left(\frac{\omega^{ki} - \omega^{kl}}{\omega^i - \omega^l} \right) F_{il} F_{li} = k\omega^{ki} \left[2\omega^{\frac{1}{m}} F_{ii} - \omega^{-i} F_{ii}^2 - \omega^{i+\frac{2}{m}} \mathbb{1} \right]. \tag{3.89}$$

Now replacing F_{ii} from Eq. (3.83) and evaluating the above relation, we arrive at

$$\sum_{\substack{l=0 \\ l\neq i}}^{d-1} \left(\frac{\omega^{ki} - \omega^{kl}}{\omega^i - \omega^l} \right) F_{il} F_{li} = -\frac{k}{d^2} \omega^{i(k+1)+\frac{2}{m}} (1 - \omega^{-d/m})^2 \mathbb{1}, \tag{3.90}$$

which can also be rewritten in the following form

$$\sum_{\substack{l=0 \\ l\neq i}}^{d-1} \left(\frac{1 - \omega^{k(l-i)}}{1 - \omega^{i-l}} \right) F_{il} F_{li} \omega^{-\left(i+l+\frac{2}{m}\right)} \omega^{\frac{d}{m}} = \frac{k}{d^2} \omega^{\frac{d}{m}} (1 - \omega^{-d/m})^2 \mathbb{1}. \tag{3.91}$$

Without loss of generality, we can replace the index l with j. Now, substituting F_{ji} from

(3.86) and also using the identity (3.84) we obtain

$$\sum_{\substack{j=0\\ j\neq i}}^{d-1}\left(\frac{1-\omega^{k(j-i)}}{1-\omega^{i-j}}\right)F_{ij}F_{ij}^{\dagger}=\frac{4k}{d^2}\sin^2\left(\frac{\pi}{m}\right)\mathbb{1}, \tag{3.92}$$

for all $k=0,\ldots,d-1$ and $i=0,\ldots,d-1$. Multiplying the above equation (3.92) with ω^{kn} such that $n=1,\ldots,d-1$, then summing over k and using the identity $\sum_{k=0}^{d-1}\omega^{kn}=0$ that holds true for any $n=1,2,\ldots,d-1$, we arrive at

$$-\sum_{\substack{j=0\\ j\neq i}}^{d-1}\frac{1}{1-\omega^{i-j}}F_{ij}F_{ij}^{\dagger}\sum_{k=0}^{d-1}\omega^{k(j-i+n)}=\frac{4}{d^2}\sin^2\left(\frac{\pi}{m}\right)\sum_{k=0}^{d-1}k\omega^{kn}\mathbb{1}. \tag{3.93}$$

Let us now consider some simple identities

$$\sum_{k=0}^{d-1}\omega^{kn}=0,\quad \text{and}\quad \sum_{k=0}^{d-1}\omega^{k(j-i)}=d\delta_{j,i} \tag{3.94}$$

which can be simply computed using the formula for the sum of geometric sequence, and,

$$\sum_{k=0}^{d-1}k\omega^{kn}=\frac{d}{\omega^n-1} \tag{3.95}$$

which has been proven in Fact 6 in Appendix A for any $n=1,\ldots,d-1$. After applying these identities to equation (3.93) we arrive at the following relation

$$F_{i(i-n \mod d)}F_{i(i-n \mod d)}^{\dagger}=\frac{4}{d^2}\sin^2\left(\frac{\pi}{m}\right)\mathbb{1}. \tag{3.96}$$

Let us notice that for a fixed i, $i-n \mod d$ covers all numbers from $\{0,\ldots,d-1\}$ except i by varying n from 1 to $d-1$. Thus, we can simply represent the above expression as

$$F_{ij}F_{ij}^{\dagger}=\frac{4}{d^2}\sin^2\left(\frac{\pi}{m}\right)\mathbb{1}. \tag{3.97}$$

Let us now consider a unitary transformation $\widetilde{V}:\mathscr{H}_1\to\mathscr{H}_1$ of the following form

$$\widetilde{V}=\sum_{i=0}^{d-1}|i\rangle\langle i|\otimes\widetilde{V}_i, \tag{3.98}$$

where $\widetilde{V}_i$ are unitary matrices acting on $\mathscr{H}_1''$ defined as

$$\widetilde{V}_0 = \mathbb{1}, \qquad \widetilde{V}_i = -\frac{d\mathbb{i}}{2\sin(\pi/m)}\omega^{-\frac{i}{2}+\frac{d-2}{2m}}F_{0i} \tag{3.99}$$

for $i = 1,\ldots,d-1$. Notice that $A_{1,2}$ remains invariant under application of $\widetilde{V}$,

$$\widetilde{V}A_{1,2}\widetilde{V}^\dagger = \widetilde{V}\left[Z_d \otimes \mathbb{1}\right]\widetilde{V}^\dagger = Z_d \otimes \mathbb{1}, \tag{3.100}$$

which a consequence of the fact that $Z_d \otimes \mathbb{1}$ commutes with $\widetilde{V}$. Applying $\widetilde{V}$ to $A_{1,3}$, we obtain

$$\widetilde{V}A_{1,3}\widetilde{V}^\dagger = \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes \tilde{F}_{ij}, \tag{3.101}$$

where we denoted $\tilde{F}_{ij} = \widetilde{V}_i F_{ij} \widetilde{V}_j^\dagger$. Notice that all the algebraic relations obtained till now for F_{ij} are equally valid for $\tilde{F}_{ij}$, and $\tilde{F}_{ii} = F_{ii}$. Employing the relation (3.97) for $i = 0$, we obtain that

$$\tilde{F}_{0j} = \widetilde{V}_0 F_{0j} \widetilde{V}_j^\dagger = \frac{d}{2}\omega^{\frac{2j+d}{4}+\frac{2-d}{2m}}F_{0j}F_{0j}^\dagger = \frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\omega^{\frac{j}{2}+\frac{2-d}{2m}}\mathbb{1}, \tag{3.102}$$

Then employing the relation between $\tilde{F}_{ij}$ and $\tilde{F}_{ji}^\dagger$ from Eq. (3.86) for $i = 0$, we obtain that $\tilde{F}_{j0} = \tilde{F}_{0j}$.

To determine the remaining matrices $F_{ij}'s$, the above relations are not enough and we also need to look at the off-diagonal elements of (3.92). For this, we again sandwich the relation (3.92) with $\langle i|.|j\rangle$ such that $i \neq j$, which leads us to

$$-(k-1)\omega^{ki}F_{ij} + \omega^{-\frac{1}{m}}\sum_{\substack{l=0\\l\neq i}}^{d-1}\left(\frac{\omega^{ki}-\omega^{kl}}{\omega^i-\omega^l}\right)F_{il}F_{lj} + k\omega^{(k-1)i}\omega^{-\frac{1}{m}}F_{ii}F_{ij} = \frac{\omega^{(k+1)i}-\omega^{(k+1)j}}{\omega^i-\omega^j}F_{ij}. \tag{3.103}$$

Plugging F_{ii} from Eq. (3.83) and then using some simple algebra, we arrive at

$$\sum_{\substack{l=0\\l\neq i}}^{d-1}\frac{\omega^{ki}-\omega^{kl}}{\omega^i-\omega^l}F_{il}F_{lj} = \omega^{\frac{1}{m}}\left[\frac{\omega^{(k+1)i}-\omega^{(k+1)j}}{\omega^i-\omega^j} + \left(\frac{(1-\omega^{-d/m})k}{d}-1\right)\omega^{ki}\right]F_{ij}. \tag{3.104}$$

Now, let us consider the above relation for $i = 0$,

$$\sum_{l=1}^{d-1}\frac{1-\omega^{kl}}{1-\omega^l}F_{0l}F_{lj} = \omega^{\frac{1}{m}}\left(\frac{1-\omega^{(k+1)j}}{1-\omega^j} + \frac{(1-\omega^{-d/m})k}{d}-1\right)F_{0j}. \tag{3.105}$$

Replacing F_{0j} as derived in (3.102),

$$\sum_{l=1}^{d-1} \frac{1-\omega^{kl}}{1-\omega^{l}} \omega^{\frac{l}{2}} F_{lj} = \omega^{\frac{j}{2}+\frac{1}{m}} \left(\frac{1-\omega^{(k+1)j}}{1-\omega^{j}} + \frac{(1-\omega^{-d/m})k}{d} - 1 \right) \mathbb{1}. \tag{3.106}$$

As the matrix F_{jj} was derived in (3.83), we separate it out from the sum on the left hand side of the above equation and replace the index l with i to finally obtain

$$\sum_{\substack{l=1 \\ l\neq j}}^{d-1} \left(\frac{1-\omega^{kl}}{1-\omega^{l}} \right) \omega^{\frac{l}{2}} F_{lj} = \frac{1-\omega^{-d/m}}{d} \omega^{\frac{j}{2}+\frac{1}{m}} \left(k + \frac{1-\omega^{kj}}{1-\omega^{j}} \omega^{j} \right) \mathbb{1}. \tag{3.107}$$

We now multiply the above relation (3.107) by ω^{-kn} with $n = 1,\ldots,d-1$ and $n \neq j$. Next, we sum the resulting relation over all k, which yields

$$\begin{aligned} &\sum_{\substack{i=1 \\ i\neq j}}^{d-1} \frac{\omega^{i/2}}{1-\omega^{i}} F_{ij} \sum_{k=0}^{d-1} \left(\omega^{-kn} - \omega^{k(i-n)} \right) \\ &\qquad = \frac{1-\omega^{-d/m}}{d} \quad \omega^{\frac{j}{2}+\frac{1}{m}} \quad \left[\sum_{k=0}^{d-1} k\omega^{-kn} + \frac{\omega^{j}}{1-\omega^{j}} \sum_{k=0}^{d-1} \left(\omega^{-kn} - \omega^{k(j-n)} \right) \right] \mathbb{1}. \end{aligned} \tag{3.108}$$

Now, exploiting the fact that $\sum_{k=0}^{d-1} \omega^{k(n-i)} = d\delta_{n,i}$ and the identity (3.95), we arrive at

$$-d \frac{\omega^{n/2}}{1-\omega^{n}} F_{nj} = \frac{1-\omega^{-d/m}}{d} \omega^{\frac{j}{2}+\frac{1}{m}} \left(\frac{d}{\omega^{-n}-1} \right) I, \tag{3.109}$$

which after rearranging some terms and replacing the index n with i, gives the matrices F_{ij} for $i \neq j$,

$$\begin{aligned} F_{ij} &= -\frac{1-\omega^{-d/m}}{d} \omega^{\frac{i+j}{2}+\frac{1}{m}} \mathbb{1} \\ &= -\frac{2\mathrm{i}\sin(\pi/m)}{d} \omega^{\frac{i+j}{2}+\frac{2-d}{2m}} \mathbb{1}, \qquad i,j = 1,\ldots,d-1, \quad i \neq j \end{aligned} \tag{3.110}$$

where to obtain the second equality, we used the identity (3.84). Combining all the derived identities, (first, F_{ii} from (3.83) for all i, second, F_{0j} and F_{j0} from (3.102) for all j and finally, the rest of the matrices F_{ij} from (3.110)) into the form of $A_{1,3}$ (3.77), we conclude that the unitary $V_1 = \widetilde{V}\overline{V}_1$,transforms $A_{1,2}$ and $A_{1,3}$ as:

$$V_1 A_{1,2} V_1^{\dagger} = Z_d \otimes \mathbb{1}, \tag{3.111}$$

and

$$V_1 A_{1,3} V_1^\dagger = T_{d,m} \otimes \mathbb{1} \tag{3.112}$$

with $T_{d,m}$ given by

$$T_{d,m} = \sum_{i=0}^{d-1} \omega^{i+\frac{1}{m}} |i\rangle\langle i| - \frac{2\mathbb{i}}{d} \sin\left(\frac{\pi}{m}\right) \sum_{i,j=0}^{d-1} (-1)^{\delta_{i,0}+\delta_{j,0}} \omega^{\frac{i+j}{2}-\frac{d-2}{2m}} |i\rangle\langle j| \tag{3.113}$$

This completes the characterisation of $A_{1,2}$ and $A_{1,3}$. □

Rest of the parties

To find the observables for rest of the parties, we follow the exact same lines as were used for finding the observables of the first party A_{1,α_1}. Let us now focus on the SOS decomposition of the Bell operator $\hat{\mathscr{B}}_{m,d,N}$ given in Eq. (3.25). As discussed before in Chapter 2 any state $|\psi_N\rangle$ belonging to the Hilbert space $\mathscr{H}_{A_1''} \otimes \ldots \otimes \mathscr{H}_{A_N''} \otimes \mathscr{H}_E$ and observables acting on it that maximally violate the Bell inequalities (3.9) must satisfy the following relations due to the SOS decomposition (3.25),

$$P^{(k)}_{n,\alpha_1,\ldots,\alpha_N} |\psi_N\rangle = 0. \tag{3.114}$$

After expanding the above expession (3.114) with the aid of Eq. (3.26), we obtain the following relation

$$A^{(k)}_{1,\alpha_1} \otimes \overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1} \otimes \bigotimes_{\substack{i=2 \\ i\neq n}}^{N} A^{(-1)^{i-1}k}_{i,\alpha_{i-1}+\alpha_i-1} |\psi_N\rangle = |\psi_N\rangle, \tag{3.115}$$

and

$$R^{(k)}_{n,\alpha} |\psi_N\rangle = 0 \tag{3.116}$$

for $k = 1,2,\ldots,d-1$, $\alpha_i = 1,2,\ldots,m$ for $i = 1,2,\ldots,N-1$, $\alpha_N = 1$ and $n = 2,3,\ldots,N$. The expressions $\overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1}$ and $R^{(k)}_{n,\alpha}$ are given in Eqs. (3.27) and (3.28) when n is odd and in Eqs. (3.29) and (3.30) when n is even. Taking into account that the local states of all the parties are full-rank, we get similar relations among the observables for every party as those in Eqs. (3.41) and (3.42) from the above expressions (3.115) and (3.116),

$$\overline{A}_{n,\alpha_{n-1}+\alpha_n-1}\ \overline{A}^\dagger_{n,\alpha_{n-1}+\alpha_n-1} = \mathbb{1}, \tag{3.117}$$

and

$$\overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1} = \left[\overline{A}^{(1)}_{n,\alpha_{n-1}+\alpha_n-1}\right]^k, \tag{3.118}$$

and

$$R^{(k)}_{n,\alpha} = 0, \tag{3.119}$$

for $k = 1,2,\ldots,d-1$, $\alpha_i = 1,2,\ldots,m$ for $i = 1,2,\ldots,N-1$, $\alpha_N = 1$ and $n = 2,3,\ldots,N$.

Let us notice that the forms of $\overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1}$ in (3.27) and (3.29) are identical to $\overline{A}_{1,\alpha_1}$. Further, $R^{(k)}_{n,\alpha}$ in (3.28) and (3.30) are identical to $R^{(k)}_{1,\alpha}$. Thus, we employ the same technique to find observables A_{n,α_n} for all n and α_n. We first use the relations (3.117) and (3.118) for $\alpha_{n-1} = 2, \alpha_n = 1$ when n is odd and $\alpha_{n-1} = 2, \alpha_n = 2$ when n is even, yielding the exactly same equations as (3.41) and (3.42) for $\alpha_1 = 2$. Thus, from Lemma 3.1 we can conclude that $\mathrm{Tr}(A^s_{n,2}) = \mathrm{Tr}(A^s_{n,3}) = 0$ for any s that is a divisor of d. Now using Fact 3 stated in Appendix B we can conclude that the multiplicity of the eigenvalues are equal. This allows us to deduce that the observables of A_n act on a Hilbert space $\mathscr{H}_n$ of dimension $d \times D_n$ where D_n is a positive integer, that is,

$$\mathscr{H}_n = \mathbb{C}^d \otimes \mathscr{H}''_n. \tag{3.120}$$

As a consequence, one can always rotate one of $A'_n s$ observables to some observable that acts on a $\mathbb{C}^d$ tensored with identity acting on $\mathscr{H}''_n$. Moreover, we can find a unitary transformation $V_n : \mathscr{H}_n \to \mathscr{H}_n$ such that

$$V_n A_{n,2} V_n^\dagger = Z_d \otimes \mathbb{1}''_n \tag{3.121}$$

where Z_d is defined in Eq. (3.32). Then, using Lemma 3.2, using the above form of $A_{n,2}$ we show that $A_{n,3}$ is also unitarily equivalent to a an observable acting on a $\mathbb{C}^d$ tensored with identity acting on $\mathscr{H}''_1$, that is,

$$V_n\ A_{n,3} V_n^\dagger = T_{d,m} \otimes \mathbb{1}''_n \tag{3.122}$$

with $T_{d,m}$ defined in Eq. (3.32). Next, we show that there exist unitary transformations $U_n : \mathscr{H}_n \to \mathscr{H}_n$ such that

$$U_n A_{n,\alpha_n} U_n^\dagger = \mathscr{O}_{n,\alpha_n} \otimes \mathbb{1}''_n \quad \text{for} \quad \alpha_1 = 2,3. \tag{3.123}$$

These unitaries U_n are explicitly calculated in Observation 3.3 stated in Appendix B.

Finally, using the derived observables and the condition (3.116) we find the rest of the observables of A_{n,α_n}. For this, we first consider the relation (3.116) for $k=1$ and $\alpha=1$. After plugging the explicit form of $R_n^{(1)}$ from (3.30) and (3.26) and then plugging the observables $A_{n,2}$ and $A_{n,3}$ from (3.123), we can easily compute that

$$U_n A_{n,4} U_n^\dagger = \mathscr{O}_{n,4} \otimes \mathbb{1}_n''. \tag{3.124}$$

The above statement can also be checked based on the fact that the ideal observables satisfy all the above conditions derived from the maximal violation of the Bell inequalities. Continuing this procedure recursively for the remaining values of α, we see that

$$U_n A_{n,\alpha_n} U_n^\dagger = \mathscr{O}_{n,\alpha_1} \otimes \mathbb{1}_n'' \qquad \forall \alpha_n. \tag{3.125}$$

This completes the characterisation of all the observables of every party. We have shown that the maximal violation of ASTA Bell inequalities (3.9) is attained only by observables that up to local unitary transformations and addditional degrees of freedom are the ideal observables (3.11), (3.12) and (3.13).

The state

We finally have all the tools required to determine the state that maximally violates the Bell inequalities (3.9). For this, we only need to consider the relation (3.41). As was derived in the previous subsection that up to a local unitary all the observables are the ideal ones. Thus, we can rewrite the relation (3.41) for $k=1$ by expanding $\overline{A}_{1,\alpha_1}^{(1)}$ as

$$\left[(a_1 \mathscr{O}_{1,\alpha_1} + a_1^* \mathscr{O}_{1,\alpha_1+1}) \otimes \bigotimes_{i=2}^{N} \mathscr{O}_{i,\alpha_{i-1}+\alpha_i-1}^{(-1)^{i-1}} \otimes \mathbb{1}'' \right] |\tilde{\psi}_N\rangle = |\tilde{\psi}_N\rangle \tag{3.126}$$

for all $\alpha_i = 1,2,\ldots,m$ such that $i=1,2,\ldots,N-1$ and $\alpha_N = 1$. Also, in the above condition $\mathbb{1}''$ acts on the Hilbert space $\mathscr{H}_1'' \otimes \mathscr{H}_2'' \otimes \ldots \otimes \mathscr{H}_N'' \otimes \mathscr{H}_E$ and

$$|\tilde{\psi}_N\rangle = U_1 \otimes U_2 \otimes \ldots \otimes U_N \otimes \mathbb{1}_E |\psi_N\rangle. \tag{3.127}$$

Let us simplify the term $a_1 \mathscr{O}_{1,\alpha_1} + a_1^* \mathscr{O}_{1,\alpha_1+1}$ by expanding it using (3.17) and (3.18),

$$\begin{aligned} a_1 \mathscr{O}_{1,\alpha} \;+\; & a_1^* \mathscr{O}_{1,\alpha+1} \\ &= \left[\sum_{i=0}^{d-2} \omega^{\gamma_m(\alpha)} \left(a_1 + a_1^* \omega^{\frac{1}{m}} \right) |i\rangle\langle i+1| + \omega^{(1-d)\gamma_2(\alpha)} \left(a_1 + a_1^* \omega^{-\frac{d-1}{m}} \right) |d-1\rangle\langle 0| \right] \otimes \mathbb{1}_n'' \\ &= \left[\sum_{i=0}^{d-2} \omega^{\zeta_m(\alpha)} |i\rangle\langle i+1| + \omega^{-(d-1)\zeta_m(\alpha)} |d-1\rangle\langle 0| \right] \otimes \mathbb{1}_n'', \end{aligned} \tag{3.128}$$

where to arrive at the third line of the above equation, we use the fact that $a_1 + a_1^* \omega^{1/m} = \omega^{1/2m}$ and $a_1 + a_1^* \omega^{-(d-1)/m} = \omega^{-(d-1)/2m}$ and also that $\gamma_m(x) + 1/2m = \zeta_m(x)$ [cf. (3.16)]. Let us now notice the action of the ideal observables on vectors belonging to the computational basis $|j\rangle$ of Hilbert space $\mathbb{C}^d$,

$$\begin{aligned} (a_1 O_{1,x} + a_1^* O_{1,x+1})|j\rangle &= \omega^{(1-d\delta_{j,0})(x/m)}|j-1\rangle, \\ \mathscr{O}_{2,x}^{-1}|j\rangle &= \omega^{-(1-d\delta_{j,0})(x/m)}|j-1\rangle, \end{aligned} \tag{3.129}$$

where the first equation follows from Eq. (3.128) and the second equation follows from (3.17). Now, when n is odd or even

$$\begin{aligned} \mathscr{O}_{n_{\text{odd}},x}|j\rangle &= \omega^{(1-d\delta_{j,0})\theta_m(x)}|j-1\rangle, \\ \mathscr{O}_{n_{\text{ev}},x}^{-1}|j\rangle &= \omega^{-(1-d\delta_{j,0})\theta_m(x)}|j-1\rangle, \end{aligned} \tag{3.130}$$

where we employed (3.18). Here, the natural convention is $|-1\rangle \equiv |d-1\rangle$.

As the local Hilbert spaces of all the parties are of the form $\mathscr{H}_i = \mathbb{C}^d \otimes \mathscr{H}_i''$, we can express the state as

$$|\tilde{\psi}_N\rangle = \sum_{i_1,\ldots,i_N=0}^{d-1} |i_1,\ldots,i_N\rangle|\psi_{i_1,\ldots,i_N,E}\rangle \tag{3.131}$$

where the vectors $|\psi_{i_1,\ldots,i_N,E}\rangle \in \mathscr{H}_1'' \otimes \ldots \otimes \mathscr{H}_N'' \otimes \mathscr{H}_E$ are in general unnormalised. Let us plug this state into the relation (3.126) for $\alpha_1 = \alpha_2 = \ldots = \alpha_N = 1$ and $k = 1$. Noting moreover that $\theta_m(1) = 0$, gives us

$$\sum_{i_1,\ldots,i_N=0}^{d-1} \omega^{\frac{d}{m}(\delta_{i_2,0}-\delta_{i_1,0})}|i_1-1\rangle\ldots|i_N-1\rangle|\psi_{i_1,\ldots,i_N,E}\rangle = \sum_{i_1,\ldots,i_N=0}^{d-1} |i_1,\ldots,i_N\rangle|\psi_{i_1,\ldots,i_N,E}\rangle, \tag{3.132}$$

where to arrive at the above expression we have also used the relations (3.129) and (3.130). Multiplying the above expression with $\langle i_1-1|\ldots\langle i_N-1|$, we obtain

$$\omega^{\frac{d}{m}(\delta_{i_2,0}-\delta_{i_1,0})}|\psi_{i_1,\ldots,i_N,E}\rangle = |\psi_{i_1-1,\ldots,i_N-1,E}\rangle \tag{3.133}$$

for all $i_1,\ldots,i_N$. Again, in the relation (3.126), we set $\alpha_1 = 2$ and $\alpha_2 = \ldots = \alpha_N = 1$ to obtain for all $i_1,\ldots,i_N$ that

$$\omega^{\frac{2d}{m}(\delta_{i_2,0}-\delta_{i_1,0})}|\psi_{i_1,\ldots,i_N,E}\rangle = |\psi_{i_1-1,\ldots,i_N-1,E}\rangle. \tag{3.134}$$

The relations (3.133) and (3.134) can be divided into two possible cases. The first case is

$\delta_{i_2,0} = \delta_{i_1,0}$ which holds true when and $i_1, i_2 = 1,2,\ldots,d-1$ or $i_1 = i_2 = 0$ for which

$$|\psi_{i_1,i_2\ldots,i_N,E}\rangle = |\psi_{i_1-1,i_2-1,\ldots,i_N-1,E}\rangle \tag{3.135}$$

and for all $i_3, i_4, \ldots, i_N$. The second case is $\delta_{i_1,0} \neq \delta_{i_2,0}$ which holds true if $i_1 = 0$ and $i_2 = 1,\ldots,d-1$ or $i_2 = 0$ and $i_1 = 1,\ldots,d-1$, for which Eq. (3.133) and Eq. (3.134) can be simultaneously satisfied if and only if

$$|\psi_{i_1,0,i_3,\ldots,i_N,E}\rangle = 0, \quad |\psi_{0,i_2,\ldots,i_N,E}\rangle = 0 \tag{3.136}$$

and for all $i_3, i_4, \ldots, i_N$. Considering (3.135) for $i_2 = 1$ and $i_1 \neq 1$, we get $|\psi_{i_1,1\ldots,i_N,E}\rangle = |\psi_{i_1-1,0,\ldots,i_N-1,E}\rangle = 0$. Again, considering (3.135) for $i_2 = 2$ and $i_1 \neq 2$, we get $|\psi_{i_2,2,\ldots,i_N,E}\rangle = |\psi_{i_1-1,1,\ldots,i_N-1,E}\rangle = 0$. Considering all the assignments of i_2 from 3 to $d-1$ in (3.135) and $i_1 \neq i_2$, we can similarly obtain that

$$|\psi_{i_1,i_2,\ldots,i_N,E}\rangle = 0 \qquad \forall i_1, i_2, \ldots, i_N \text{ s.t. } i_1 \neq i_2 \tag{3.137}$$

and,

$$|\psi_{i_2-1,i_2-1,i_3-1,\ldots,i_N-1,E}\rangle = |\psi_{i_2,i_2,i_3,\ldots,i_N,E}\rangle \qquad \forall i_2, i_3, \ldots, i_N. \tag{3.138}$$

We again consider the relations (3.126) for $\alpha_1 = \alpha_3 = \ldots = \alpha_N = 1$ and $\alpha_2 = 2$. Using the above derived condition (3.137), we can focus only on the cases when $i_1 = i_2$ as rest of the terms are 0. Due to this we arrive at the following condition for all $i_2, \ldots, i_N$,

$$\omega^{\frac{d}{m}(\delta_{i_2,0}-\delta_{i_3,0})}|\psi_{i_2,i_2,i_3\ldots,i_N,E}\rangle = |\psi_{i_2-1,i_2-1,i_3-1,\ldots,i_N-1,E}\rangle. \tag{3.139}$$

Again, there are two posible solutions when simultaneously solving Eq. (3.138) and the above Eq. (3.139). The first solution is that $\delta_{i_2,0} = \delta_{i_3,0}$ which holds true for $i_2, i_3 = 1,2,\ldots,d-1$ or $i_2 = i_3 = 0$ for which

$$|\psi_{i_2,i_2,i_3,\ldots,i_N,E}\rangle = |\psi_{i_2-1,i_2-1,i_3-1,\ldots,i_N-1,E}\rangle \tag{3.140}$$

and for all $i_4, i_5 \ldots, i_N$. The second solution is that $\delta_{i_3,0} \neq \delta_{i_2,0}$ which holds true if $i_3 = 0$ and $i_2 = 1,\ldots,d-1$ or $i_2 = 0$ and $i_3 = 1,\ldots,d-1$, for which

$$|\psi_{0,0,i_3,\ldots,i_N,E}\rangle = 0, \quad |\psi_{i_2,i_2,0,\ldots,i_N,E}\rangle = 0 \tag{3.141}$$

and for all $i_4, i_5 \ldots, i_N$. Considering the above equation (3.140) for $i_2 = 1$ and $i_3 \neq 1$, we obtain that $|\psi_{1,1,i_3,\ldots,i_N,E}\rangle = |\psi_{0,0,i_3,\ldots,i_N-1,E}\rangle = 0$, Again, considering the above equation

(3.140) for $i_2 = 2$ and $i_3 \neq 2$, we obtain that $|\psi_{2,2,i_3,\ldots,i_N,E}\rangle = |\psi_{1,1,i_3,\ldots,i_N-1,E}\rangle = 0$. Considering all the assignments of i_2 from 3 to $d-1$ in (3.140) and $i_3 \neq i_2$, we can similarly obtain that

$$|\psi_{i_2,i_2,i_3,\ldots,i_N,E}\rangle = 0 \qquad \forall i_2, i_3, \ldots, i_N \text{ s.t. } i_2 \neq i_3 \tag{3.142}$$

and,

$$|\psi_{i_2-1,i_2-1,i_2-1,\ldots,i_N-1,E}\rangle = |\psi_{i_2,i_2,i_2,\ldots,i_N,E}\rangle \qquad \forall i_2, i_4, \ldots, i_N. \tag{3.143}$$

Proceeding in a similar manner, we assign $\alpha_n = 2$ for any $n = 3,4,\ldots,N-1$ with the rest of coefficients as $\alpha_1 = \alpha_2 = \alpha_3 = \ldots = \alpha_N = 1$ in Eq. (3.126), we obtain $N-3$ different conditions. We solve them exactly the same way as was done for $n = 2$, and can finally conclude that the only non-zero terms among $|\psi_{i_1,i_2,i_3,\ldots,i_N,E}\rangle$ are related as,

$$|\psi_{i-1,i-1,i-1,\ldots,i-1,E}\rangle = |\psi_{i,i,i,\ldots,i,E}\rangle \quad \forall i. \tag{3.144}$$

Thus, we can conclude from (3.131) that

$$|\tilde{\psi}_N\rangle = \sum_{i=0}^{d-1} |ii\ldots i\rangle \otimes |\psi_{0,0,\ldots,0,E}\rangle. \tag{3.145}$$

Normalising the state, we can rewrite it as

$$U_1 \otimes \ldots \otimes U_N |\psi_N\rangle = \left(\frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes N}\right) \otimes |\tilde{\psi}_{0,0,\ldots,0,E}\rangle \tag{3.146}$$

where $|\tilde{\psi}_{0,0,\ldots,0}\rangle = 1/\sqrt{d}|\psi_{0,0,\ldots,0,E}\rangle$. Thus, the state that maximally violates the Bell inequalities (3.9) up to some local unitaries is infact the generalised GHZ state (3.1) along with some uncorrelated auxiliary state on which the measurements act trivially. This finally completes the proof of our self-testing scheme. □

3.4 Randomness certification

As was discussed before in introduction Chapter 2, self-testing of quantum states and measurements can be used to design methods of certification of genuine randomness that can be generated using the outcomes of the measurement device. Even if some external attacker Eve has access to the measurement devices and the state, self-testing restricts the maximum probability by which Eve can guess the generated outputs.

For this, let us consider the scenario in which one of the observers, say the first

party A_1, wishes to generate randomness using the outcomes of their measurements. As discussed before, Eve might supply the measurement devices which might give some predetermined outputs that are known to her. Interestingly, the self-testing scheme presented in this Chapter can be used to certify $\log_2 d$ bits of perfect randomness in the outcomes of any measurement of any party. Let us now focus on A_1's measurements, keeping in mind that the results apply to any party. We compute the probability of Eve to guess the measurement outcomes of A_1's. For this, we refer to the local guessing probability (2.147) introduced in Chapter 2 which can be straightforwardly extended to the multipartite scenario,

$$G(\alpha_1,\vec{\mathbf{p}}) = \sup_{S_p} \sum_b \langle \psi_N | Q_{\alpha_1}^{(b)} \otimes \mathbb{1}_{A_2} \otimes \ldots \otimes \mathbb{1}_N \otimes E^{(b)} | \psi_N \rangle, \tag{3.147}$$

where $|\psi_N\rangle \in \mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \ldots \otimes \mathscr{H}_N \otimes \mathscr{H}_E$ is the N-partite state shared by all the parties as well as Eve. Here $Q_{\alpha_1}^{(b)}$ is the $b-$th projector corresponding to the α_1-th measurement performed by A_1, and $E^{(b)}$ corresponds to the $b-$th outcome of a d-outcome measurement performed by Eve on her share of the state. This is Eve's best guess of A_1's outcome. Finally, S_p is the set of all possible strategies that Eve can use to guess of A_1's measurement outputs.

Let us consider that all the parties perform the Bell test on a state $|\psi\rangle$ and observe the maximal violation of the Bell inequalities (3.9). As concluded in the previous section, up to local unitary operations, the quantum state is given by (3.146) and the measurement operators of A_1's can be expressed as $Q_{\alpha_1}^{(b)} = \bar{Q}_{\alpha_1}^{(b)} \otimes \mathbb{1}_{A''}$, where $\bar{Q}_{\alpha_1}^{(b)}$ are eigenprojectors of the ideal observables (3.11). Going back to the local guessing probability (3.147), which can be rewritten as

$$G(\alpha_1,\vec{\mathbf{p}}) = \sup_{S_p} \sum_b \mathrm{Tr}\left(Q_{\alpha_1}^{(b)} \otimes E^{(b)} \rho_{A_1 E}\right) \tag{3.148}$$

where $\rho_{A_1 E} = \mathrm{Tr}_{A_2 A_3 \ldots A_N}(|\psi_N\rangle\langle\psi_N|)$. From (3.146), we obtain the following density matrix

$$\rho_{A_1 E} = \frac{1}{d} \sum_{i=0}^{d-1} |i\rangle\langle i| \otimes \rho_{A_1'' E}. \tag{3.149}$$

Plugging the above state and measurement $Q_{\alpha_1}^{(b)}$ to the guessing probability (3.148), we arrive at

$$G(\alpha_1,\vec{\mathbf{p}}) = \frac{1}{d} \sup_{S_p} \sum_b \sum_i \langle i | Q_{\alpha_1}^{(b)} | i \rangle \mathrm{Tr}\left(\mathbb{1}_{A_1''} \otimes E^{(b)} \rho_{A_1'' E}\right) \tag{3.150}$$

Notice that $\sum_i \langle i|Q_{\alpha_1}^{(b)}|i\rangle = 1$ for any b, which allows us to finally arrive at

$$\begin{aligned} G(\alpha_1,\vec{\mathbf{p}}) &= \frac{1}{d}\sup_{S_p}\sum_b \mathrm{Tr}\left(\mathbb{1}_{A_1''}\otimes E^{(b)}\rho_{A_1''E}\right) \\ &= \frac{1}{d} \end{aligned} \tag{3.151}$$

where we used the fact that Eve performs a valid measurement and thus $\sum_b E^{(b)} = \mathbb{1}_E$ and $\mathrm{Tr}(\rho_{A_1''E}) = 1$. Thus, we can certify $-\log_2 G(\alpha_1,\vec{\mathbf{p}}) = \log_2 d$ bits of randomness from the maximal violation of the Bell inequalities (3.9). The same analysis can be extended to any party.

3.5 Conclusions and discussions

We proposed the first self-testing scheme for the certification of generalised GHZ state that relies on violation of a single Bell inequality and requires only two measurements per observer. Apart from this our approach relies on the maximum violation of a Bell inequality that involves $d-$outcome measurements. The previous approach to self-test the generalised GHZ state in Ref. [25] extends the scheme of Ref. [32] by utilising the maximum violation of the tilted CHSH inequality [144] by considering two dimensional subspaces among two parties. Here the first party needs to perform three and the rest of the parties need to perform four measurements each. Unlike this approach, our method does not rely on self-testing results for two-dimensional systems. We propose a novel mathematical approach to derive self-testing statements. Moreover, our scheme is experimentally friendly as we can self-test generalised GHZ states using the minimal number of measurements required to observe Bell nonlocality, that is, two. This makes our scheme more practical and easier to implement experimentally as compared to [32] because it reduces the amount of data necessary to certify the devices. As a matter of fact, violation of the SATWAP Bell inequalities has been experimentally demonstrated in Ref. [153] for $d = 3$. Our scheme can also be considered as a generalisation of the self-testing scheme based on chained Bell inequalities [16] to quantum systems of an arbitrary local dimension as well as arbitrary number of parties.

We also showed that our scheme can be used to securely generate the maximum amount of randomness using projective measurements with arbitrary number of outcomes. This result is also interesting from a foundational point of view as this is the first instance, where a single measurement can be used to generate genuine unbounded randomness with the highest possible security. Our self-testing scheme has also been exploited in Ref. [154] to show that the set of quantum correlations in a certain Bell scenario is not closed.

An interesting follow-up of our work was presented in [155], [156] where correlations of constant size where enough to self-test any two-qudit maximally entangled state.

Our work provokes some follow up problems. The first interesting problem would be to devise an analytic technique that can also give information about the state and measurements even when one does not obtain the exact quantum bound but a value slightly lower than it. The only analytical method to derive such robustness bounds is restricted to scenarios where the parties perform two-outcome measurements [12], [13], [19], [20]. For the SATWAP Bell inequalities, in Ref. [39] the robustness was derived for $d = 3$ and $m = 2$ using the numerical approach based on semi-definite programming. Such results would be particularly important for experimental implementations.

Another interesting problem would be to derive genuinely $d-$outcome Bell inequalities that are maximally violated by partially entangled states in the bipartite case and other classes of multipartite entangled states such as $W-$states and then explore whether these inequalities can be used for self-testing. As was discussed in introduction, the maximum amount of randomness that one can generate using a $d-$dimensional system is of amount $2\log_2 d$ bits using non-projective measurements. Thus, it would be interesting to see whether our self-testing scheme can be used to certify this optimal randomness along the lines of Refs. [41], [42] which consider qubit and qutrit states respectively.

Chapter 4

Certification of incompatible measurements

4.1 Introduction

Most of the self-testing schemes aims to certify quantum states without much emphasis on measurements even when one of the necessary conditions for existence of non-classical correlations can be attributed to the presence of incompatible measurements in quantum theory. Moreover, self-testing of quantum measurements in the Bell scenario has restrictions as was shown in [157], [158]. Specifically, there exist pair of incompatible measurements that do not violate any Bell inequality. As a consequence, it might not be possible to certify every pair of incompatible measurements in a fully device-independent way and therefire it is reasonable to look for scenarios that are weaker than the Bell scenario. One such possibility is to assume that one of the parties in the Bell experiment is fully characterised and performs known measurements. This is the well-known quantum steering scenario. As a matter a fact, it was recently proven that there is a one-to-one correspondence between quantum steering and measurement incompatibility [159]–[161], suggesting that every pair of incompatible measurements can be certified in a steering scenario. This makes quantum steering well suited for our task of certifying incompatible measurements. Certification using quantum steering was proposed recently [51], [52] but only for qubits and for a specific pair of 2-outcome measurements. It is worth noting that, the technique used in these schemes [51], [52] cannot be used to certify arbitrary pair of 2-outcome incompatible measurements.

We provide here a simple scheme for certification of d-outcome incompatible projective measurements and the maximally entangled state of local dimension d. Our scheme can be used to certify a family of quantum observables termed here "genuinely incompatible".

Roughly speaking, genuinely incompatible observables are those that do not share a common invariant proper subspace [see below for a precise definition]. For instance, mutually unbiased bases (MUBs) acting on d-dimensional Hilbert spaces are genuinely incompatible. Inspired by the inequalities presented in Refs. [162], [163], we introduce a family of steering inequalities that are maximally violated by the maximally entangled state and any set of genuinely incompatible measurements. We analyse the case when this inequality can be maximally violated by measurements that are not genuinely incompatible. We also study the robustness of our certification scheme towards experimental imperfections when trusted Alice chooses a pair of mutually unbiased bases to measure her subsystem.

4.2 Family of steering inequalities

Let us first recall the quantum steering scenario introduced in Chapter 2 in an analogous way to Bell scenario. Alice and Bob are located in spatially separated labs. Both of them receive two unknown subsystems from a preparation device. Alice is trusted and performs N known $d-$outcome measurements on the received subsystem. On the other hand, Bob also performs N $d-$outcome measurements on his subsystem but these measurements are unknown. The measurements of both Alice and Bob are labelled by $x,y = 1,2,\ldots,N$ whereas the outcomes as $a,b = 0,1,\ldots,d-1$. They collect enough statistics to construct the joint probability distribution $\{p(a,b|x,y)\}$. The scenario is depicted in Fig. 4.1.

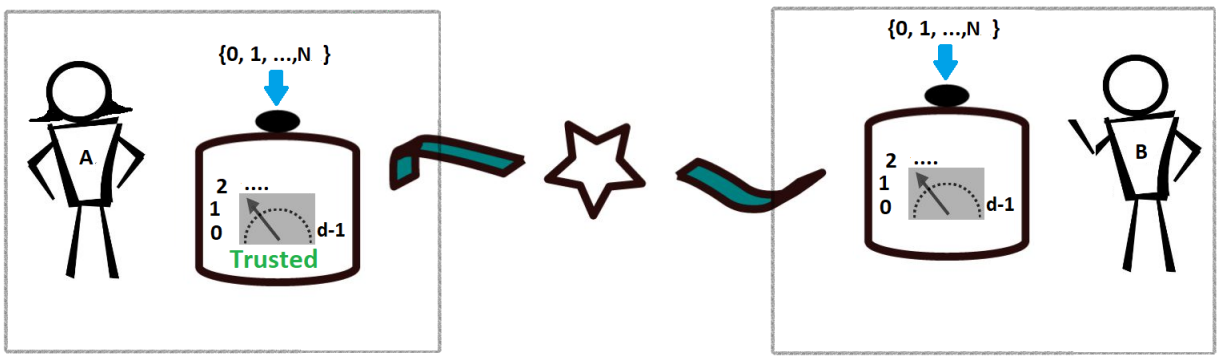


Figure 4.1: Quantum steering scenario: Alice and Bob both receive a system from the preparation device on which each of them perform N $d-$outcome measurements such that N,d are integers greater than or equal to two. The experiment is repeated enough number of times to generate the relevant joint probability distribution. The key difference between this and Bell scenario is that Alice is trusted and her measurements are known.

Inspired by [162], [163], we construct the following family of steering inequalities written using generalised observables [cf. Sec. 2.1.3] as

$$W_{2,d,N} = \sum_{k=1}^{d-1} \sum_{y=1}^{N} \left\langle A_y^k \otimes B_{k|y} \right\rangle \leq \beta_L. \tag{4.1}$$

Note that the steering functional in the above expression looks similar to (2.73), here however we assume that the observables $A_{k|x}$ are unitary, that is, $A_{k|x} = A_x^k$. We also moved the term for $k = 0$ to the classical bound, as it simply reduces to the expectation value of $\mathbb{1}$ which is one. Alice is trusted and thus A_y are known to act on Hilbert space of dimension d. Recall that Bob's measurements act on a Hilbert space of unknown but finite dimension. The above steering functional (4.1) can also be expressed in terms of joint probabilities as

$$W_{2,d,N} = d \sum_{x=1}^{N} \sum_{a,b=0}^{d-1} c_{a,b}\ p(a,b|x,y=x) - N, \tag{4.2}$$

where,

$$c(a,b,x,y) = \begin{cases} 1 & \text{if} \quad a \oplus_d b = 0 \\ 0 & \text{otherwise} \end{cases} \tag{4.3}$$

where $a \oplus_d b$ represents $a+b$ modulo d. To get from the observable picture (4.1) to the joint probability picture (4.2), we used the relation (2.18) from Chapter 2, that is,

$$\langle A_{k|x} \otimes B_{l|y} \rangle = \sum_{a,b=0}^{d-1} \omega^{(ka+lb)} p(a,b|x,y) \tag{4.4}$$

for all k,l,x,y. Let us now compute the classical bound β_L of the steering functional in Eq. (4.1).

4.2.1 Classical bound

As discussed in Chapter 2, the classical bound of the steering functional (4.1) can be calculated by assuming that the assemblage $\{\sigma_{b|y}\}$ admits a local hidden state model, that is,

$$\sigma_{b|y} = \sum_{\lambda} p(\lambda) p(b|y,\lambda) \rho_\lambda, \tag{4.5}$$

where λ represents the hidden variables that are distributed with probability $p(\lambda)$, $p(b|y,\lambda)$ denotes the probability of obtaining outcome b when Bob performs the mea-

surement y given the hidden variable λ and ρ_λ are hidden states that act on Alice's Hilbert space. Using (4.5), the corresponding joint probabilities $p(a,b|x,y)$ for assemblages admitting a LHS model are given by

$$p(a,b|x,y) = \mathrm{Tr}(M_{a|x}\sigma_{b|y}) = \sum_\lambda p(\lambda)p(b|y,\lambda)\mathrm{Tr}(M_{a|x}\rho_\lambda), \tag{4.6}$$

where $M_{a|x}$ represents the projector corresponding to the outcome a when Alice performs the measurement x. The above expression can also be stated as

$$p(a,b|x,y) = \sum_\lambda p(\lambda)p(a|x,\rho_\lambda)p(b|y,\lambda), \tag{4.7}$$

where $p(a|x,\rho_\lambda) = \mathrm{Tr}(M_{a|x}\rho_\lambda)$. Now, using the joint probability form of the steering functional (4.2), we have that

$$W_{2,d,N} = d\sum_{x=1}^{n}\sum_{a,b=0}^{d-1}\sum_\lambda c_{a,b}\ p(\lambda)p(a|x,\rho_\lambda)p(b|x,\lambda) - N \tag{4.8}$$

where $c_{a,b}$ is given in (4.3). Thus, the steering functional simplifies to

$$W_{2,d,N} = d\sum_{x=1}^{N}\sum_{a=0}^{d-1}\sum_\lambda p(\lambda)p(a|x,\rho_\lambda)p(d-a|x,\lambda) - N. \tag{4.9}$$

The above term is upper bounded by

$$\sum_{x=1}^{N}\sum_a\sum_\lambda p(\lambda)p(a|x,\rho_\lambda)p(d-a|x,\lambda) \leq \sum_{x=1}^{N}\sum_\lambda p(\lambda)\max_a\{p(a|x,\rho_\lambda)\} \tag{4.10}$$

where we used the normalisation condition $\sum_a p(a|x,\lambda) = 1$ and then the fact that for any real-valued function $f(x) \in \mathbb{R}$,

$$\sum_a p(a)f(a) \leq \max_a f(a) \qquad \text{such that} \qquad \sum_a p(a) = 1. \tag{4.11}$$

Also, notice that

$$\sum_{x=1}^{N}\sum_\lambda p(\lambda)\max_a\{p(a|x,\rho_\lambda)\} \leq \sum_{x=1}^{N}\max_\rho\sum_\lambda p(\lambda)\max_a\{p(a|x,\rho)\}. \tag{4.12}$$

Now, using the fact that $\sum_\lambda p(\lambda) = 1$, we obtain an upper bound on the value of the steering functional as

$$W_{2,d,N} \leq d \sum_{x=1}^{N} \max_{\rho} \max_{a} \{p(a|x,\rho)\} - N \tag{4.13}$$

Doing an inverse Fourier transform and expressing in terms of expectation values, we have

$$W_{2,d,N} \leq \sum_{x=1}^{N} \max_{\rho} \max_{a} \sum_{k=1}^{d-1} \omega^{-ka} \left\langle \hat{A}_x^k \right\rangle_\rho \leq \sum_{x=1}^{N} \max_{\rho} \sum_{k=1}^{d-1} \left| \left\langle \hat{A}_x^k \right\rangle_\rho \right|. \tag{4.14}$$

Thus, we conclude that the local bound of $W_{2,d,N}$ is upper bounded by,

$$\beta_L \leq \sum_{i=1}^{N} \max_{\rho} \sum_{k=1}^{d-1} \left| \left\langle \hat{A}_i^k \right\rangle_\rho \right|. \tag{4.15}$$

This bound can be explicitly calculated for different set of observables A_x. For instance, if $N = d = 2$ and $A_1 = \sigma_z$ and $A_2 = \sigma_x$ (2.27) then the classical bound is given by $\beta_L = \sqrt{2}$. Let us consider the special case, when $N = 2$ such that $A_1 = Z_d$ and $A_2 = X_d$ which are the $d-$dimensional generalisation of the Pauli matrices σ_z and σ_x respectively whose explicit form is given below in Eq. (2.91). In this case, the classical bound is given by $\beta_L = \sqrt{2}(d-1)$ and was computed in [162]. Let us now compute the quantum bound of the steering functional in Eq. (4.1).

4.2.2 Quantum bound

It is straightforward to find the maximal quantum bound of the steering functional (4.1). Let us first note that the algebraic bound of (4.1) is $N(d-1)$ and can be achieved when each term of the functional equals one. Let us now consider the maximally entangled state of two qudits,

$$|\phi_+^d\rangle = \frac{1}{\sqrt{d}} \sum_i |ii\rangle, \tag{4.16}$$

and Bob's observables are unitary and conjugate of Alice's observables, that is, $B_y = A_y^*$ for all y. For these quantum realisations, the expectation value of every term in the functional (4.1) is one. Thus the quantum bound of the steering functional (4.1) is same as its algebraic bound, that is,

$$\beta_Q = N(d-1). \tag{4.17}$$

Consequently, the quantum state and the measurements that achieve the maximum quantum value β_Q of the steering functional (4.1) for fixed observables A_i must satisfy the

following relations

$$\langle A_y^k \otimes B_{k|y} \rangle = 1 \qquad \forall y,k. \tag{4.18}$$

Since A_y is unitary and $B_{k|y}^\dagger B_{k|y} \leq \mathbb{1}$, for any state ρ_{AB} that satisfies the above relation, we have that

$$A_y^k \otimes B_{k|y} \rho_{AB} = \rho_{AB} \qquad \forall y,k. \tag{4.19}$$

This relation would be particularly useful for deriving the 1SDI certification results.

Let us now figure out the cases when the steering inequality $W_{2,d,N} \leq \beta_L$ is non-trivial, that is $\beta_L < \beta_Q$. For this, let us see when the upper bound (4.15) to the value attainable using classical strategies is equal to the quantum bound, that is,

$$\sum_{i=1}^{N} \sum_{k=0}^{d-1} |\langle A_i^k \rangle_\rho| = N(d-1). \tag{4.20}$$

This implies that each term in the above relation is 1 or simply $|\langle A_i^k \rangle_\rho| = 1$ for all i, k and ρ acting on $\mathbb{C}^d$. Let us say that ρ admits a decomposition in terms of pure states as $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Since A_i^k are unitary operators, this means that $|\psi_i\rangle$ are the eigenvectors of all A_i with eigenvalues of modulus 1. Thus, we can conclude that for the steering inequality to be non-trivial the observables A_i cannot share any common eigenvector. However, the steering functional (4.1) can not be used to certify all such observables that do not share a common eigenvector, but a restricted set of such observables termed as "genuinely incompatible" observables. The reason for this ambiguity would be clarified in the later sections.

4.3 Genuinely incompatible observables

Here we refer to the definition of genuine incompatible (GI) observables introduced in [62].

Definition 1 (Genuine incompatible observables)**.** *Consider a set of N d-outcome unitary observables A_i acting on $\mathbb{C}^d$ and obeying $A_i^d = \mathbb{1}$. We call them genuinely incompatible (GI) if there is no subspace $V \subset \mathbb{C}^d$ such that $\dim V < d$ and $A_i V \subseteq V$ for all i; in other words, the only common invariant space of all A_i is the full space $\mathbb{C}^d$.*

Let us recall the $d-$outcome observables introduced in Chapter 2 in Eq. (2.91):

$$Z_d = \sum_{i=0}^{d-1} \omega^i |i\rangle\langle i|, \qquad X_d = \sum_{i=0}^{d-1} |i+1\rangle\langle i| \tag{4.21}$$

that are $d-$dimensional generalisation of the Pauli matrices σ_z, σ_x (2.27). Note that in the above sum $|i+1\rangle$ is modulo d. The eigenvectors of these observables are mutually unbiased (see Def. 2 below). These observables are genuinely incompatible.

Definition 2 (Mutually unbiased bases)**.** *Two orthonormal bases* $\{|e_i^0\rangle\}$ *and* $\{|e_i^1\rangle\}$ *in* $\mathbb{C}^d$ *form mutually unbiased bases if*

$$|\langle e_i^0|e_j^1\rangle|^2 = \frac{1}{d} \tag{4.22}$$

for every $i, j = 0, 1, \ldots, d-1$.

We then say that two unitary observables A_0 and A_1 are mutually unbiased if their eigenvectors are mutually unbiased. There are a few interesting observations about GI observables.

1. Two $d-$outcome observables A_0 and A_1 are not genuinely incompatible if there exist a basis in $\mathbb{C}^d$ using which the observables can be decomposed as

$$A_0 = A_0' \oplus A_0'' \quad \text{and} \quad A_1 = A_1' \oplus A_1'' \tag{4.23}$$

   such that A_0' and A_1' act on a $d'-$dimensional subspace of $\mathbb{C}^d$ with $d' < d$. In this case, the observables share a common invariant subspace $\mathbb{C}_{d'}$ spanned by the eigenvectors of A_0' (or equivalently, the eigenvectors of A_1').

2. Genuinely incompatible observables do not share a common eigenvector. We verify this claim after Lemma 4.1 stated below. Thus, when Alice's observables are genuinely incompatible, the steering inequality (4.1) $W_{2,d,N} \leq \beta_L$ is non-trivial

3. Consider a set of N observables. If this set contains two observables that are GI, then the whole set is genuinely incompatible as well. This is because if two observables do not share a common invariant subspace, then any set containing these two observables can not share any invariant subspace.

4. The opposite implication of the above statement is not true. Set of observables might be genuinely incompatible even when pairwise they are not genuinely incompatible.

To illustrate the above statement with an example, let us consider three five-outcome observables with eigenvalues ω^i with $x = 0, 1, 2, 3, 4$, such that $\omega = \exp(\frac{2\pi \mathrm{i}}{5})$, written in the computational basis.

$$A_0 = \frac{1}{2}\begin{pmatrix} 1+\omega & 1-\omega & 0 & 0 & 0 \\ 1-\omega & 1+\omega & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & 0 & \omega^4 \end{pmatrix},$$

$$A_1 = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & \omega^2+\omega & \omega^2-\omega & 0 & 0 \\ 0 & \omega^2-\omega & \omega^2+\omega & 0 & 0 \\ 0 & 0 & 0 & 2\omega^3 & 0 \\ 0 & 0 & 0 & 0 & 2\omega^4 \end{pmatrix},$$

$$\text{and} \qquad A_2 = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & f_1(\omega,\omega_3) & f_2(\omega,\omega_3) & f_3(\omega,\omega_3) \\ 0 & 0 & f_3(\omega,\omega_3) & f_1(\omega,\omega_3) & f_2(\omega,\omega_3) \\ 0 & 0 & f_2(\omega,\omega_3) & f_3(\omega,\omega_3) & f_1(\omega,\omega_3) \end{pmatrix} \tag{4.24}$$

where $f_1(\omega,\omega_3) = \omega^2+\omega^3+\omega^4$, $f_2(\omega,\omega_3) = \omega^2+\omega_3^2\omega^3+\omega_3\omega^4$ and $f_3(\omega,\omega_3) = \omega^2+\omega_3\omega^3+\omega_3^2\omega^4$ such that $\omega_3 = \exp(\frac{2\pi\mathbb{i}}{3})$. Let us first find the eigenvectors of the above observables. The eigenvectors of $A_0's$ are $\{|+_{01}\rangle,|-_{01}\rangle,|2\rangle,|3\rangle,|4\rangle\}$, second, $A_1's$ eigenvectors are $\{|0\rangle,|+_{12}\rangle,|-_{12}\rangle,|3\rangle,|4\rangle\}$ and finally, $A_2's$ eigenvectors are $\{|0\rangle,|1\rangle,|e_1\rangle,|e_2\rangle,|e_3\rangle\}$ where $|\pm_{ij}\rangle = (|i\rangle \pm |j\rangle)/\sqrt{2}$ and

$$|e_1\rangle = \frac{1}{\sqrt{3}}(|2\rangle+|3\rangle+|4\rangle), \quad |e_2\rangle = \frac{1}{\sqrt{3}}\left(|2\rangle+\omega_3|3\rangle+\omega_3^2|4\rangle\right),$$
$$\text{and} \quad |e_3\rangle = \frac{1}{\sqrt{3}}\left(|2\rangle+\omega_3^2|3\rangle+\omega_3|4\rangle\right). \tag{4.25}$$

From Lemma 4.1 which is stated below, we conclude that A_0 and A_1 have two non-trivial common invariant subspaces, spanned by $\{|0\rangle,|1\rangle,|2\rangle\}$ and $\{|3\rangle,|4\rangle\}$. Again, A_0 and A_2 have two non-trivial common invariant subspaces, spanned by $\{|0\rangle,|1\rangle\}$ and $\{|2\rangle,|3\rangle,|4\rangle\}$. Finally, A_1 and A_2 have two non-trivial common invariant subspaces, spanned by $\{|0\rangle\}$ and $\{|1\rangle,|2\rangle,|3\rangle,|4\rangle\}$. Thus, if we consider the pair of the above observables, none of such pairs are genuinely incompatible. However, considering all three observables, we can readily see that there is no common invariant subspace shared between A_0, A_1 and A_2 as we simultaneously cannot express all the matrices using blocks of dimension less than 5×5.

Now, we prove a lemma that would be useful for characterising genuinely incompatible observables.

Lemma 4.1. *Two $d-$outcome observables A_0 and A_1 share a common non-trivial invariant subspace of dimension $d' < d$ if and only if d' eigenvectors of A_0 can be expressed as a linear combination of d' eigenvectors of A_1.*

Proof. Let us first recall that two $d-$outcome observables A_0 and A_1 share a common invariant subspace if there exist a basis in $\mathbb{C}^d$ using which the observables can be decomposed as

$$A_0 = A_0' \oplus A_0'' \quad \text{and} \quad A_1 = A_1' \oplus A_1'' \tag{4.26}$$

such that A_0' and A_1' act on d' dimensional Hilbert space where $d' < d$. The common invariant subspace is $\mathbb{C}_{d'}$ and is spanned by the d' eigenvectors of A_0' or the d' eigenvectors of A_1'. Thus, eigenvectors of A_0' can be expressed as linear combination of eigenvectors of A_1' as they span the same Hilbert space. We showed here that if A_0 and A_1 share a common invariant subspace of dimension d', then d' eigenvectors of A_0 can be written as d' eigenvectors of d'.

It is trivial to show the other way round, that is, if d' eigenvectors of A_0 can be written as d' eigenvectors of A_1, then A_0 and A_1 share a common invariant subspace spanned by these eigenvectors. This ends the proof. □

Note that if two observables share a common eigenvector, then they share a common invariant subspace of dimension one. Thus, genuinely incompatible observables can not even share a common eigenvector. A corollary of the above lemma is that mutually unbiased bases are genuinely incompatible.

Corollary. *Any two d-outcome observables whose eigenbases form mutually unbiased bases, are genuinely incompatible.*

Proof. Consider two $d-$element mutually unbiased bases denoted by, $\{|s_i\rangle\}$ and $\{|t_j\rangle\}$ such that $|\langle s_i|t_j\rangle|^2 = 1/d$ for all $i, j \in \{0, 1, \ldots, d-1\}$. One can construct $d-$outcome observables whose eigenbases are mutually unbiased in the following way,

$$A_0 = \sum_{i=0}^{d-1} \omega^i |s_i\rangle\langle s_i|, \qquad A_1 = \sum_{i=0}^{d-1} \omega^i |t_i\rangle\langle t_i|. \tag{4.27}$$

where $\omega = \exp\left(\frac{2\pi \mathrm{i}}{d}\right)$. Any eigenvector $|s_i\rangle$ of A_0 can only be written as a linear combination of all the d eigenvectors $|t_j\rangle$ of A_1. Thus, from Lemma 4.1 we have that for A_0 and A_1 do not share a non-trivial common invariant subspace and therefore are genuinely incompatible. □

Another important property of genuinely incompatible observables which is particularly useful for 1SDI certification is stated below.

Lemma 4.2. *Consider a set of N d-outcome unitary observables A_y with eigenvalues ω^i for $i = 0,1,\ldots,d-1$ such that $\omega = \exp(\frac{2\pi\mathbb{i}}{d})$. Consider also a non-trivial normal matrix P acting on $\mathbb{C}^d$. If $[P,A_y] = 0$ for every $y = 1,2,\ldots,N$ such that the set of observables A_y are genuinely incompatible, then $P = \lambda\mathbb{1}_d$ where λ is an arbitrary complex number.*

Proof. The proof is by contradiction, that is, we assume that $P \neq \lambda\mathbb{1}_d$. Let us first note that since P is normal, there exists a unitary that transforms P to a diagonal matrix. Thus, we can always express P, in terms of its orthogonal projections P_i and the corresponding eigenvalues λ_i, in the following way

$$P = \sum_{i=1}^{m} \lambda_i P_i. \tag{4.28}$$

Here $\lambda_i's$ are distinct complex numbers that might be even 0 and m denotes the number of such distinct eigenvalues.

Let us now assume that $[P,A_y] = 0$ for all y. Expanding this relation, we have that

$$A_y\ P = P\ A_y. \tag{4.29}$$

Let us now consider two orthogonal projections P_m and P_n of P such that $m \leq n$. Now, we multiply P_m from left hand side and P_n from the right hand side of the above equation (4.29) to obtain

$$P_m\ A_y\ P\ P_n = P_m\ P\ A_y\ P_n. \tag{4.30}$$

Using the fact that $P_iP_j = \delta_{ij}$ in (4.28), we have that $PP_n = \lambda_nP_n$ and $P_mP = \lambda_mP_m$. This allows us to simplify the above equation (4.30) as

$$(\lambda_m - \lambda_n)P_m\ A_y\ P_n = 0. \tag{4.31}$$

The above equation has two possible solutions:

$$\lambda_m = \lambda_n \quad \text{or} \quad P_m\ A_y\ P_n = 0. \tag{4.32}$$

For distinct m,n, the eigenvalues λ_m,λ_n are also distinct. Thus, we conclude that $P_m\,A_i\,P_n = 0$ whenever $m \neq n$. This means that A_y decomposes into blocks that act on $\mathrm{supp}(P_i)$. We can obtain the same conclusion for every observable A_y. Given that P and A_y satisfy the relation $[P,A_y] = 0$ for all y, if P is of the form (4.28), then all $A_y's$ are of the block form

$$A_y = A_y^{(1)} \oplus \ldots \oplus A_y^{(m)}. \tag{4.33}$$

This contradicts the fact that $A_y's$ are genuinely incompatible which implies that $P = \lambda \mathbb{1}_d$ for some $\lambda \in \mathbb{C}$. Notice that the trivial solution to the condition $[P, A_y] = 0$ is when $P = 0$. Any non-trivial solution such that A_y are genuinely incompatible observables imposes that the rank of P is d and all its eigenvalues are equal and non-zero. This ends the proof. □

Finally, we have all the required tools for deriving the results concerning certification of incompatible measurements.

4.4 1SDI certification

4.4.1 Exact certification of GI observables

Here, we present the 1SDI certification of genuinely incompatible measurements that relies on maximal violation of the steering inequality (4.1) $W_{2,d,N} = \beta_Q$. Let us first recall that we can only characterise Bob's observables on the support of his local state ρ_B. Thus, without loss of generality we can consider that the local state ρ_B is full rank. This can also be understood as that Bob's observables and local state ρ_B act on the same Hilbert space $\mathscr{H}_B$.

Theorem 4.1. *Consider that Alice and Bob perform the quantum steering experiment and observe that the steering functional*

$$W_{2,d,N} = \sum_{k=1}^{d-1} \sum_{y=1}^{N} \left\langle A_y^k \otimes B_{k|y} \right\rangle, \tag{4.34}$$

attains the maximal quantum value $\beta_Q = N(d-1)$ where N is number of measurements performed by Alice and Bob and d denotes the number of outcomes of each measurement. Alice's observables A_y acting on $\mathbb{C}^d$ are unitary with eigenvalues ω^i such that $\omega = \exp(\frac{2\pi \mathbb{i}}{d})$ and are genuinely incompatible. Let us say that the maximal quantum bound is achieved using the state ρ_{AB} acting on $\mathbb{C}^d \otimes \mathscr{H}_B$ and Bob's generalised observables B_i $(i \in \{1, \ldots, N\})$ acting on $\mathscr{H}_B$. Then, the following statements hold true for any integer d greater than or equal to two:

1. *Bob's measurements are projective. Equaivalently, the operators $B_{k|y}$ for all k, y are unitary and $B_{k|y} = B_{1|y}^k \equiv B_y^k$.*

2. *Bob's Hilbert space $\mathscr{H}_B$ admits a decomposition into a $d-$dimensional Hilbert space $\mathbb{C}^d)_{B'}$ and an auxiliary Hilbert space of unkown but finite dimension $\mathscr{H}_{B''}$,*

$$\mathscr{H}_B = (\mathbb{C}^d)_{B'} \otimes \mathscr{H}_{B''}. \tag{4.35}$$

3. *A local unitary transformation* $U_B : \mathscr{H}_B \to \mathscr{H}_B$ *can be applied on Bob's side, such that*

$$(\mathbb{1}_A \otimes U_B)\rho_{AB}(\mathbb{1}_A \otimes U_B^\dagger) = |\phi_d^+\rangle\langle\phi_d^+|_{AB'} \otimes \rho_{B''}. \tag{4.36}$$

where $|\phi_d^+\rangle$ *is the maximally entangled state* (4.16) *and*

$$\forall y, \quad U_B B_y U_B^\dagger = A_y^* \otimes \mathbb{1}_{B''}, \tag{4.37}$$

where B'' *denotes Bob's auxiliary system.*

Proof. Let us first recall the relations (4.19) that stem from the fact that to saturate the quantum bound of the steering functional (4.1) each of the expectation values in the functional must amount to one,

$$A_y^k \otimes B_{k|y}\rho_{AB} = \rho_{AB} \tag{4.38}$$

for $y = 1,2,\ldots,N$ and $k = 1,2,\ldots,d-1$. We begin by showing that the above relations can only be satisfied if Bob's measurements are projective. Note that an equivalent representation of the above relation (4.38) is

$$A_y^{d-k} \otimes B_{d-k|y}\rho_{AB} = \rho_{AB} \qquad \forall y,k. \tag{4.39}$$

Recall that by definition $B_{d-k|y} = B_{k|y}^\dagger$ [cf. (2.22)]. Now, multiplying (4.38) with $A_y^{d-k} \otimes B_{d-k|y}$, we have that

$$\left(A_y^{d-k}A_y^k \otimes B_{d-k|y}B_{k|y}\right)\rho_{AB} = \left(A_y^{d-k} \otimes B_{d-k|y}\right)\rho_{AB} \qquad \forall y,k. \tag{4.40}$$

Using the fact that $A_y^d = \mathbb{1}_A$ and the relation (4.39), we have that

$$\left(\mathbb{1}_A \otimes B_{k|y}^\dagger B_{k|y}\right)\rho_{AB} = \rho_{AB}. \tag{4.41}$$

Tracing over the subsystem A, we get that

$$\left(B_{k|y}^\dagger B_{k|y}\right)\rho_B = \rho_B \tag{4.42}$$

and since ρ_B is full-rank and thus invertible, we finally have that $B_{k|y}^\dagger B_{k|y} = \mathbb{1}_B$ for all k,y such that $\mathbb{1}_B$ is the identity acting on $\mathscr{H}_B$. Similarly, taking the relation (4.39) and multiplying it with $A_y^k \otimes B_{k|y}$, we get that $B_{k|y}B_{k|y}^\dagger = \mathbb{1}_B$ for all k,y such that $\mathbb{1}_B$. Thus, one straightforwardly concludes from the above conditions that $B_{k|y}$ are unitary for every y

and k. Now using Fact 1, we conclude that Bob's measurements are projective. Since, for projective measurements $B_{k|y} = B_y^k$, from here on we substitute $B_{k|y} = B_y^k$.

Let us focus on the state ρ_{AB} that results in the quantum bound of the steering functional (4.34). Consider the eigendecomposition of ρ_{AB} as

$$\rho_{AB} = \sum_{s=1}^{K} p_s |\psi_s\rangle\langle\psi_s|_{AB}, \tag{4.43}$$

where K is any integer greater than or equal to one and $p_s \geq 0$ such that $\sum_s p_s = 1$. Further, the eigenstates $|\psi_s\rangle$ are pairwise orthogonal, that is, $\langle\psi_s|\psi_{s'}\rangle = \delta_{ss'}$ for every s, s'.

First, we show that the rank of the local state of Alice is d. The proof is by contradiction. For this, we use the relations (4.38) and the fact that Alice's observables A_i are genuinely incompatible. Let us assume that rank of ρ_A is strictly less than d. Then, we consider the relation (4.19) for $k = 1$ and then project Alice's observables onto the support of the state ρ_A,

$$\Pi_A A_y \Pi_A \otimes B_y \ \rho_{AB} = \rho_{AB}, \tag{4.44}$$

where Π_A is the projector onto the support of Alice's local state ρ_A. Let us denote $\overline{A}_i \equiv \Pi_A A_i \Pi_A$. Also, considering the relation (4.39) for $k = 1$, we have that

$$\Pi_A A_y^\dagger \Pi_A \otimes B_y^\dagger \ \rho_{AB} = \rho_{AB}. \tag{4.45}$$

Note, that $\Pi_A A_y^\dagger \Pi_A = (\Pi_A A_y \Pi_A)^\dagger$. As proven above, Bob's measurements that result in the maximal violation are projective and thus B_y are unitary and satisfy $B_y^d = \mathbb{1}$. Now, applying $\overline{A}_y \otimes B_y$ to the equation (4.45), we have that

$$\left(\overline{A}_y \overline{A}_y^\dagger \otimes B_y B_y^\dagger\right) \rho_{AB} = \rho_{AB}. \tag{4.46}$$

Again, using the fact that B_y are unitary and then taking a trace of subsystem B, we have that

$$\overline{A}_y \overline{A}_y^\dagger = \Pi_A \tag{4.47}$$

As proven in Fact 4 in Chapter 2, since $\overline{A}_y$ is unitary , it must be of block form

$$A_y = \overline{A}_y \oplus A'_y \tag{4.48}$$

for some unitary matrix A'_y of dimension $[d - \text{rank}(\rho_A)] \times [d - \text{rank}(\rho_A)]$. However, from Lemma 4.1 we conclude that $A'_y s$ have a common invariant subspace of dimension lower

$\text{rank}(\rho_A)$ which strictly lower than d. This contradicts the fact that A_y are genuinely incompatible observables. As a consequence, ρ_A is a full rank matrix, or equivalently the rank of the local state of Alice ρ_A is d.

Now, we have all the required tools to formulate the main part of the theorem which includes characterising the state ρ_{AB} and Bob's observables B_y that result in the quantum bound of the steering functional (4.34). Let us first expand the relation (4.38) using the decomposition of the state ρ_{AB} (4.43) keeping in mind that Bob's observables are projective,

$$\sum_{s=1}^{K} p_s \, A_y^k \otimes B_y^k |\psi_s\rangle\langle\psi_s|_{AB} = \sum_{s=1}^{K} p_s |\psi_s\rangle\langle\psi_s|_{AB} \qquad \forall y,k. \tag{4.49}$$

Multiplying with $|\psi_s\rangle$ on the right hand side of the above equation, we arrive at the following condition,

$$A_y^k \otimes B_y^k |\psi_s\rangle_{AB} = |\psi_s\rangle_{AB} \qquad \forall s,y,k \tag{4.50}$$

where we used the fact that $\langle\psi_s'|\psi_s\rangle = \delta_{ss'}$ for every s,s'.

Now, we can characterise every $|\psi_s\rangle$ and then find the relation among them to fully identify the state ρ_{AB}. Let us first note from the relation (4.50) that Bob's measurements acting on the support of the local state $\rho_{B,s} = \text{Tr}_A(|\psi_s\rangle\langle\psi_s|_{AB})$ are also projective. For this we can follow the exactly same procedure as was done in the beginning of the proof to conclude that B_y acting on the support of ρ_B is projective. Thus, we can conclude that

$$B_y = \Pi_B^s B_y \Pi_B^s \oplus E_s \tag{4.51}$$

where Π_B^s represents the projector onto the support of $\rho_{B,s}$ and E_s is some unitary matrix. For completeness, let us briefly discuss the proof again. We begin by considering the relations (4.38) and (4.39) for $k=1$ and project it onto the support of $\rho_{B,s}$, that is,

$$A_y \otimes \overline{B}_{y,s} |\psi\rangle_{AB} = |\psi_s\rangle_{AB} \quad \text{and} \quad A_y^\dagger \otimes \overline{B}_{y,s}^\dagger |\psi\rangle_{AB} = |\psi_s\rangle_{AB} \tag{4.52}$$

where $\overline{B}_{y,s} = \Pi_B^s B_y \Pi_B^s$. By applying $A_y \otimes \overline{B}_{y,s}$ to the left equation in (4.52) $d-1$ times, we obtain that $\overline{B}_{y,s}^d = \mathbb{1}_d$. Now, applying $A_y^\dagger \otimes \overline{B}_{y,s}^\dagger$ to the right equation in (4.52) of the above equation, we conclude that $\overline{B}_{y,s}^\dagger \overline{B}_{y,s} = \mathbb{1}_d$. Similarly, we can also conclude that $\overline{B}_{y,s} \overline{B}_{y,s}^\dagger = \mathbb{1}_d$. As a result $\overline{B}_{y,s}$ are unitary and thus represent projective measurements with eigenvalues $\{1, \omega, \ldots, \omega^{d-1}\}$. Using the Fact 4 proven in Chapter 2, we finally arrive at the desired block form of Bob's observables (4.51).

Since all the states $|\psi_s\rangle_{AB}$ follow the same relation (4.50), foe the moment let us drop

the index s and consider a simple state $|\psi\rangle_{AB}$. As concluded before in Lemma 4.2, when the set of observables A_y are genuinely incompatible, $\mathbf{rank}(\rho_A) = d$ which implies that the local dimension of the state is d. This allows us to consider the Schmidt decomposition of $|\psi\rangle_{AB}$ as

$$|\psi\rangle_{AB} = \sum_{i=0}^{d-1} \lambda_i |e_i\rangle|f_i\rangle. \tag{4.53}$$

As ρ_A is of full-rank, the Schmidt coefficients λ_i for $(i = 0, \ldots, d-1)$ are all strictly greater than zero. Also, the normalisation of the state $|\psi\rangle_{AB}$ relates the coefficients by the condition $\sum_i \lambda_i^2 = 1$. Moreover, the local vectors $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ form two orthonormal bases in $\mathbb{C}^d$.

Let us now consider a unitary $U_B : \mathbb{C}^d \to \mathbb{C}^d$ such that $|f_i\rangle = U_B^\dagger |e_i^*\rangle$ for every i, where the asterisk denotes complex conjugation in the computational basis. Applying this unitary to the state (4.53), we have that

$$(\mathbb{1}_A \otimes U_B)|\psi\rangle_{AB} = \sum_{i=0}^{d-1} \lambda_i |e_i\rangle|e_i^*\rangle. \tag{4.54}$$

Now, let us consider a diagonal matrix P_A with eigenvectors $\{|e_i\rangle\}$ and eigenvalues $\sqrt{d}\,\lambda_i$, that is, $P_A = \sqrt{d}\lambda_i \sum_{i=0}^{d-1} |e_i\rangle\langle e_i|$. Now, the state (4.53) can be written as

$$(\mathbb{1}_A \otimes U_B)|\psi\rangle_{AB} = (P_A \otimes \mathbb{1}_B)\frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |e_i\rangle|e_i^*\rangle \tag{4.55}$$

Recall that all $\lambda_i' s$ are positive real numbers which implies that P_A is full rank, or equivalently $\mathbf{rank}(P_A) = d$. Notice that the state on the right hand side of (4.55) is the two-qudit maximally entangled state (4.16) as there exist a unitary $V : \mathbb{C}^d \to \mathbb{C}^{\mathrm{d}}$ such that $V|i\rangle = |e_i\rangle$. Let us now perform following operation

$$V \otimes V^* \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |e_i\rangle|e_i^*\rangle. \tag{4.56}$$

Now using the Fact 5, we arrive at $V \otimes V^*|\phi_d^+\rangle = VV^\dagger \otimes \mathbb{1}|\phi_d^+\rangle = |\phi_d^+\rangle$. Thus, the two-qudit maximally entangled state remains invariant under the action of the unitary of the form $V \otimes V^*$. As a consequence, we finally arrive at the simplified version of the state (4.53) given by

$$(\mathbb{1}_A \otimes U_B)|\psi\rangle_{AB} = (P_A \otimes \mathbb{1}_B)|\phi_d^+\rangle. \tag{4.57}$$

Substituting the above state (4.57) to the relation (4.50) for $k = 1$, we obtain that

$$(A_y P_A \otimes \widetilde{B}_y)|\phi_d^+\rangle = (P_A \otimes \mathbb{1}_B)|\phi_d^+\rangle, \tag{4.58}$$

where $\widetilde{B}_y = U_B^\dagger \overline{B}_y U_B$. Again, employing Fact 5 stated in Appendix A which states that Thus, we finally arrive at

$$(A_y P_A \widetilde{B}_y^T \otimes \mathbb{1}_B)|\phi_d^+\rangle = (P_A \otimes \mathbb{1}_B)|\phi_d^+\rangle. \tag{4.59}$$

Now, taking the partial trace over subsystem B, we arrive at

$$A_y P_A \widetilde{B}_y^T = P_A. \tag{4.60}$$

Multiplying the above equation with its hermitian conjugate from the right hand side, we arrive at

$$\left(A_y P_A \widetilde{B}_y^T\right)\left(\widetilde{B}_y^* P_A A_y^\dagger\right) = P_A^2, \tag{4.61}$$

where we used the fact that P_A is hermitian, that is, $P_A = P_A^\dagger$. Recalling that $\widetilde{B}_y$ are unitary allows us to conclude that

$$\widetilde{B}_y^T \widetilde{B}_y^* = (\widetilde{B}_y^\dagger \widetilde{B}_y)^* = \mathbb{1}_d \tag{4.62}$$

and thus from (4.61) we finally arrive at

$$A_y \; P_A^2 \; A_y^\dagger = P_A^2. \tag{4.63}$$

Using the fact that A_y are unitary, we arrive at a simple condition for P_A that for every y the commutator of A_y and P_A^2 is zero, that is, $[A_y, P_A^2] = 0$. Since, $P_A \geq 0$, this condition is equivalent to

$$[A_y, P_A] = 0 \quad \forall y. \tag{4.64}$$

Taking into account that A_y are genuinely incompatible, Lemma 4.2 implies that P_A is proportional to identity or simply $P_A = \lambda \mathbb{1}_A$ for some $\lambda \in \mathbb{C}$. Plugging this form of P_A into Eq. (4.60) we deduce that

$$\widetilde{B}_y = U_B \overline{B}_y U_B^\dagger = A_y^* \tag{4.65}$$

Let us now go back to every state $|\psi_s\rangle_{AB}$ and reconsider the condition (4.50). Now as concluded above for a particular s, there exist a local transformation $U_{B,s} : \mathbb{C}^d \to \mathbb{C}^d$ for every s that transforms Bob's observables acting on the support of $\rho_{B,s}$ as

$$\widetilde{B}_{y,s} = U_{B,s} \overline{B}_{y,s} U_{B,s}^\dagger = A_y^*. \tag{4.66}$$

Also, from (4.55) we get that up to a local transformation the state $|\psi_s\rangle_{AB}$ is the two-qudit

maximally entangled state

$$(\mathbb{1}_A \otimes U_{B,s})|\psi_s\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |e_i\rangle|e_i^*\rangle = |\phi_+^d\rangle. \tag{4.67}$$

Let us notice that the unitary transformation $U_{B,s}$ might be different for different s. Moreover, they also act on different subspaces of Bob's local Hilbert space. In the last part of the proof, we show that these subspaces are mutually orthogonal and thus we arrive at the form of state ρ_{AB} as (4.36) and Bob's measurement as (4.37). For this, let us first rewrite the state $|\psi_s\rangle_{AB}$ (4.67) as

$$|\psi_s\rangle_{AB} = [\mathbb{1} \otimes (U_{B,s})^\dagger]|\phi_+^d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |e_i'\rangle|g_{i,s}\rangle, \tag{4.68}$$

where the vectors $|g_{i,s}\rangle = (U_{B,s})^\dagger|e_i'^*\rangle$ form an orthonormal basis in $\mathbb{C}^d$ for any s. Note that for convenience, we expressed the state (4.68) in the eigenbasis of A_0 given by $\{|e_i'\rangle\}$. This is well justified as the two-qudit maximally entangled state remains invariant under application of the unitary $V \otimes V^*$ as shown above. The support of the local state $\rho_{B,s}$ is spanned by the vectors $|g_{i,s}\rangle$, that is,

$$\text{supp}(\rho_{B,s}) \equiv V_s = \text{span}\{|g_{0,s}\rangle, |g_{1,s}\rangle, \ldots, |g_{d-1,s}\rangle\} \subset \mathscr{H}_B. \tag{4.69}$$

Now, we show that all the local subspaces V_s corresponding to the eigenstates $|\psi_s\rangle_{AB}$ of ρ_{AB} (4.43) are mutually orthogonal. To this end, let us consider two arbitrary eigenstates, for simplicity denoted by $|\psi_1\rangle_{AB}$ and $|\psi_2\rangle_{AB}$ and the corresponding local subspaces on Bob's side as V_1 and V_2. Let us now express Alice's observable A_0 using its eigendecomposition as $A_0 = \sum_{i=0}^{d-1} \omega^i |e_i'\rangle\langle e_i'|$. For simplicity, in the rest of the proof we denote $|e_i'\rangle$ as $|i\rangle$. Plugging A_0 and the certified state (4.68) to the relation (4.50) for $y = 0$, $s = 1,2$ and $k = 1$, we have that

$$\sum_{i=0}^{d-1} \omega^i |i\rangle\langle i| \otimes B_0 \left(\frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|g_{i,s}\rangle \right) = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|g_{i,s}\rangle \qquad s = 1,2. \tag{4.70}$$

Multiplying $\langle i|$ from the left hand side of the above equation, we have that

$$B_0|g_{i,s}\rangle = \omega^{-i}|g_{i,s}\rangle \qquad s = 1,2. \tag{4.71}$$

Thus, we clearly observe that both local bases $\{|g_{i,1}\rangle\}$ and $\{|g_{i,2}\rangle\}$ are the eigenbases of B_0.

Recalling that B_0 is unitary, we find some orthogonality relations among the vectors

of the two bases specifically that eigenvectors corresponding to different eigenvalues must be orthogonal

$$\langle g_{i,1}|g_{j,2}\rangle = 0 \qquad (i \neq j). \tag{4.72}$$

As a consequence, to prove that V_1 is orthogonal to V_2, it is now enough to show that eigenvectors corresponding to same eigenvalues are also orthogonal, or equivalently

$$\langle g_{i,1}|g_{j,2}\rangle = 0 \quad \forall i,j. \tag{4.73}$$

To this end, we consider the decomposition of the vectors belonging to subspace V_2 in terms of vectors belonging to V_1 kepping in mind the condition (4.72) as

$$|g_{i,2}\rangle = \alpha_i|g_{i,1}\rangle + \beta_i|h_i\rangle, \tag{4.74}$$

where $\alpha_i, \beta_i \in \mathbb{C}$ and $|\alpha_i|^2 + |\beta_i|^2 = 1$ and $|h_i\rangle$ is a normalized vector orthogonal to $|g_{i,1}\rangle$ for any i. Again, using the condition (4.72), we clearly observe from Eq. (4.74) that

$$\beta_j\langle g_{i,1}|h_j\rangle = 0 \qquad (i,j = 0,\ldots,d-1). \tag{4.75}$$

The above equation has two possible solutions, either $\beta_j = 0$ or the vectors $|h_j\rangle$ are orthogonal to the whole subspace V_1.

Let us now revisit the conditions (4.50) for $k = 1$, $y = 2,3,\ldots,N$ and $s = 1,2$ written as

$$(\mathbb{1}_A \otimes B_y)|\psi_s\rangle_{AB} = (A_y^\dagger \otimes \mathbb{1}_B)|\psi_s\rangle_{AB} \quad s = 1,2. \tag{4.76}$$

Using then the certified state $|\psi_s\rangle_{AB}$ given in Eq. (4.68) we have that

$$\sum_{i=0}^{d-1} |i\rangle \otimes (B_y|g_{i,s}\rangle) = \sum_{i=0}^{d-1} (A_y^\dagger|i\rangle) \otimes |g_{i,s}\rangle. \tag{4.77}$$

Multiplying with $\langle i|$ on both sides of the above equation, we arrive at the following set of vector equations

$$B_y|g_{i,s}\rangle = \sum_{m=0}^{d-1} \langle i|A_y^\dagger|m\rangle|g_{m,s}\rangle \qquad s = 1,2. \tag{4.78}$$

for $i = 0,\ldots,d-1$. Using the decomposition (4.74) in (4.78) for $s = 2$, leads us to

$$\alpha_i B_y|g_{i,1}\rangle + \beta_i B_y|h_i\rangle = \sum_{m=0}^{d-1} \alpha_m\langle i|A_y^\dagger|m\rangle|g_{m,1}\rangle + \sum_{m=0}^{d-1} \beta_m\langle i|A_i^\dagger|m\rangle|h_m\rangle. \tag{4.79}$$

Now, using Eq. (4.78) for $s=1$ and substituting $B_y|g_{i,1}\rangle$ we have that

$$\sum_{m=0}^{d-1}(\alpha_i-\alpha_m)\langle i|A_y^\dagger|m\rangle|g_{m,1}\rangle=\sum_{m=0}^{d-1}\beta_m\langle i|A_y^\dagger|m\rangle|h_m\rangle-\beta_i B_y|h_i\rangle. \tag{4.80}$$

Multiplying the above equation with $\langle g_{n,1}|$ on the left hand side, we obtain

$$(\alpha_i-\alpha_n)\langle i|A_y^\dagger|n\rangle=-\beta_i\langle g_{n,1}|B_y|h_i\rangle, \tag{4.81}$$

where we used that $\beta_m\langle g_{n,1}|h_m\rangle=0$ for any n,m (4.75). Again, using the condition (4.75) along with the property of B_y acting invariantly on the subspace spanned by $|g_{n,1}\rangle$. This can also inferred from (4.78) and thus the right-hand side of the above equation simply vanishes and we finally arrive at

$$(\alpha_i-\alpha_n)\langle i|A_y^\dagger|n\rangle=0\qquad(i,n=0,\ldots,d-1). \tag{4.82}$$

Now, consider a matrix $Q=\sum_{i=0}^{d-1}\alpha_i|i\rangle\langle i|$ and observe that the left hand side of the above condition can be expressed as the commutator of $A_y^\dagger$ and Q,

$$[A_y^\dagger,Q]=0\quad\forall y \tag{4.83}$$

However, using the fact that A_y are genuinely incompatible and Lemma 4.1, the above condition can only hold if $Q=\alpha\mathbb{1}$ for some $\alpha\in\mathbb{C}$. This means that all $\alpha_i's$ are equal.

Let us now recall that the eigenstates $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal and thus using (4.68), we arrive at

$$0=\langle\psi_1|\psi_2\rangle=\frac{1}{d}\sum_i\langle g_{i,1}|g_{k,2}\rangle=\frac{1}{d}\sum_i\alpha_i=\alpha. \tag{4.84}$$

As $\alpha_i\geq 0$, we have that $\alpha_i=\alpha=0$ for any i. Plugging it back to Eq. (4.74), we can clearly observe that $|g_{i,2}\rangle=\beta_i|h_i\rangle$ such that $\beta_i=\exp(\mathbb{i}\theta_i)$. Finally, from (4.74) the inner product $\langle g_{i,2}|g_{i,1}\rangle=\alpha=0$. Thus, we can finally say that the subspaces V_1 and V_2 are mutually orthogonal. Applying the same argument by considering every pair of subspaces V_j and V_k, allows us to conclude that every pair of the subspaces are mutually orthogonal. Thus, Bob's Hilbert space decomposes as

$$\mathscr{H}_B=V_1\oplus V_2\oplus\ldots\oplus V_K, \tag{4.85}$$

where each subspace V_s is of dimension d, that is, $\dim V_s=d$. Equivalently, Bob's Hilbert space can be represented as $\mathscr{H}_B=(\mathbb{C}^d)_{B'}\otimes\mathscr{H}_{B''}$ for some Hilbert space $\mathscr{H}_{B''}$ of unknown

but finite dimension. Another consequence of the subspaces V_s being mutually orthogonal is that we can construct a unitary $U_B : \mathscr{H}_B \to \mathscr{H}_B$ such that

$$U_B|g_{i,s}\rangle = |i\rangle_{B'} \otimes |s\rangle_{B''}, \tag{4.86}$$

for $i = 0,\ldots,d-1$ and $s = 1,\ldots,K$ such that $|s\rangle$ is the computational basis over $\mathscr{H}_{B''}$. Thus, the states $|\psi_s\rangle_{AB}$ transform as

$$(\mathbb{1}_A \otimes U_B)|\psi_s\rangle_{AB} = |\phi_+^d\rangle_{AB'} \otimes |s\rangle_{B''} \tag{4.87}$$

for every s. Let us now look at the state ρ_{AB} and use the decomposition (4.43) to get that

$$(\mathbb{1}_A \otimes U_B)\rho_{AB}(\mathbb{1}_A \otimes U_B^\dagger) = |\phi_+^d\rangle\langle\phi_+^d| \otimes \rho_{B''}, \tag{4.88}$$

such that $\rho_{B''} = \sum_s p_s|s\rangle\langle s|_{B''}$. Note that $|s\rangle_{B''}$ is the eigenbasis of $\rho_{B''}$ This is exactly the form of the state we wanted to prove (4.36). To find the desired form of Bob's observables (4.37), we first notice that applying U_B (4.86) to Bob's observables B_y gives us

$$U_B B_y U_B^\dagger = \sum_{s,t=1}^{K} B_{y,s,t} \otimes |s\rangle\langle t|_{B''}, \tag{4.89}$$

where $B_{y,s,t}$ are $d \times d$ blocks acting on $(\mathbb{C}^d)_{B'}$. Plugging Eqs. (4.88) and (4.89) into Eq. (4.38) for $k = 1$ and also recalling that Bob's measurements are projective, we obtain

$$\sum_{s,t}(A_y \otimes B_{y,s,t})|\phi_+^d\rangle\langle\phi_+^d| \otimes p_t|s\rangle\langle t|_{B''} = |\phi_+^d\rangle\langle\phi_+^d| \otimes \sum_s p_s|s\rangle\langle s|_{B''}. \tag{4.90}$$

Sandwiching the above equation with $\langle s|.|t\rangle$, we get that for $s \neq t$

$$(A_y \otimes B_{y,s,t})|\phi_+^d\rangle = 0. \tag{4.91}$$

Since, A_y is unitary, we can clearly see that $B_{y,s,t} = 0$ for $s \neq t$. The terms of (4.90) for $s = t$ gives us

$$(A_y \otimes B_{y,s,s})|\phi_+^d\rangle = |\phi_+^d\rangle. \tag{4.92}$$

Due to Fact 5 proven in Appendix A, we have that $B_{y,s,s} = A_i^*$ which on substitution to Eq. (4.89), finally gives us the exact form of Bob's observables (4.37)

$$U_B B_i U_B^\dagger = \sum_{s=1}^{K} A_i^* \otimes |s\rangle\langle s|_{B''} = A_i^* \otimes \mathbb{1}_{B''}. \tag{4.93}$$

This ends the proof. □

4.4.2 Weaker certification

Let us now consider the quantum steering scenario as described above when the set of Alice's observables are not genuinely incompatible observables and thus they share a common invariant subspace. In this case, the saturation of the quantum bound (4.1) is insufficient to certify the Bob's full observable but only the part of it which acts on these subspaces. For example, consider two four-outcome observables on Alice's side as,

$$A_1 = \sum_{j=0}^{3} (\mathbb{i})^j |j\rangle\langle j|, \qquad A_2 = \sum_{j=0}^{1} (-1)^j \left(|-_j\rangle\langle -_j| + \mathbb{i}^{j+1}|+_j\rangle\langle +_j|\right) \tag{4.94}$$

where $|\pm_0\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, $|\pm_1\rangle = (|2\rangle \pm |3\rangle)/\sqrt{2}$. Any diagonal matrix P_A of the form

$$P_A = \left(\begin{array}{c|c} \lambda_1 \mathbb{1}_2 & \mathbb{O} \\ \hline \mathbb{O} & \lambda_2 \mathbb{1}_2 \end{array}\right)$$

satisfies the commutation relation $[P_A, A_y] = 0$ for $y = 1,2$ given in (4.94). Consequently, any bipartite state of local dimension four of the form

$$|\psi_{AB}\rangle = \lambda_1(|00\rangle + |11\rangle) + \lambda_2(|22\rangle + |33\rangle) \tag{4.95}$$

such that $\lambda_1^2 + \lambda_2^2 = 1$ gives the quantum bound of the steering functional (4.1). Bob's observables can be certified on the subspace where the coefficients $\lambda_i \neq 0$. For instance, when Alice's observables are given in (4.94), then the quantum bound of steering functional (4.1) can achieved by the two-qubit maximally entangled state and Bob's observbales are given by $B_1 = |0\rangle\langle 0| - \mathbb{i}|1\rangle\langle 1|$ and $B_2 = |-_0\rangle\langle -_0| - \mathbb{i}|+_0\rangle\langle +_0|$. Thus, neither Bob's observables nor the state shared among the parties can be exactly certified if the set of observables on the trusted side are not genuinely incompatible.

4.4.3 Robust certification

Let us now study the robustness of our certification scheme against experimental defects that might not lead to achieving the exact quantum bound but a value little lower than it. A numerical approach was suggested in [140], where a general scheme to robustly certify steerable assemblage was devised using the semi-definite programming. However, this approach is not applicable in our case because we consider systems of arbitrary local dimension d. A more challenging task would be to find analytical methods to address the considered problem. Here we find a simple technique to find robustness bounds of certification in the quantum steering scenario, when the trusted side chooses a family of genuinely $d-$outcome incompatible observables that are mutually unbiased

bases. Specifically, the proof given below works when the steering functional is given by (4.1) and the Alice's observables are $A_1 = X_d Z_d^l$ with $l = 0,\ldots,d-1$ and $A_2 = Z_d$. Unlike our exact certification scheme, for simplicity we assume here that the underlying state is pure and Bob's observables zare projective. These two assumptions are well justified in a non-cryptographic scenario where there is no Eve who has access to the untrusted lab as well as the preparation device. In this scenario, the states and the measurements can always be purified by extending the Hilbert space of the untrusted party.

Theorem 4.2. *Consider that Alice and Bob perform the quantum steering experiment and observe that the steering functional $W_{d,2}$ [(4.1) for $N = 2$] attains a value close to the quantum bound $\beta_Q = 2(d-1)$, that is,*

$$W_{d,2} = \sum_{k=1}^{d-1}\sum_{y=1}^{2} \left\langle A_y^k \otimes B_y^k \right\rangle \geq 2(d-1) - \varepsilon, \tag{4.96}$$

such that Bob's measurements are projective and Alice's observables are given by $A_1 = X_d Z_d^l$ with $l = 0,1,\ldots,d-1$ and $A_2 = Z_d$. Let us say that this value is attained by the state $|\psi_{AB}\rangle \in \mathbb{C}^d \otimes \mathscr{H}_B$ and observables B_y $(i = 1,2)$, that are unitary with eigenvalues $1,\omega,\ldots,\omega^{d-1}$, acting on $\mathscr{H}_B$. Then, for any integer d greater than or equal to two, there exist a unitary $U_B : \mathscr{H}_B \to \mathscr{H}_B$ such that:

1. *The state $|\psi_{AB}\rangle$ is close to the ideal state $|\phi_+^d\rangle$ up to a function of ε, that is,*

$$\left\| (\mathbb{1}_A \otimes U_B)\,|\psi_{AB}\rangle - |\phi_d^+\rangle \right\| \leq \sqrt{2(3d+1)}\sqrt[4]{2\varepsilon}. \tag{4.97}$$

2. *Bob's observables are close to the ideal Bob's observables up to a function of ε, that is,*

$$\left\| U_B B_1^k U_B^\dagger - (X_d Z_d^{-l})^k \right\|_2 \leq \sqrt{d}\left(\sqrt{2\varepsilon} + 2\sqrt{2(3d+1)}\sqrt[4]{2\varepsilon}\right) \tag{4.98}$$

and,

$$\left\| U_B B_2^k U_B^\dagger - Z_d^{-k} \right\|_2 \leq \sqrt{d}\left(\sqrt{2\varepsilon} + 2\sqrt{2(3d+1)}\sqrt[4]{2\varepsilon}\right) \tag{4.99}$$

with $k = 0,\ldots,d-1$ and $\|\cdot\|_2$ stands for the Hilbert-Schmidt norm.

Proof. Let us first manipulate the condition (4.96) to obtain a few inequalities that are crucial for the proof. As A_y, B_y are unitary, the absolute value of its expectation values are bounded by one due to which we have that $\mathrm{Re}\left(\langle A_y^k \otimes B_y^k\rangle\right) \leq \left|\langle A_y^k \otimes B_y^k\rangle\right| \leq 1$ for all y,k. Further as discussed before, the maximum value of the expectation values in the steering

functional (4.96) is one. Thus, for every $y = 1,2$ and $k = 1,2,\ldots,d-1$ we have that

$$\mathrm{Re}\left(\langle A_y^k \otimes B_y^k\rangle\right) + 2d - 3 \geq 2d - 2 - \varepsilon \tag{4.100}$$

which on simplification yields us that

$$\left|\langle\psi|A_y^k \otimes B_y^k|\psi\rangle\right| \geq \mathrm{Re}\left(\langle\psi|A_y^k \otimes B_y^k|\psi\rangle\right) \geq 1 - \frac{\varepsilon}{2} \geq 1 - \varepsilon. \tag{4.101}$$

Here, we also used the fact the absolute value of a complex number is always greater than or equal to its real value, that is, $|z| \geq \mathrm{Re}(z)$ for any complex number z.

Another observation that is important in our proof is that any bipartite state $|\psi\rangle$ of local dimension d can be expressed in the computational basis as,

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle|b_i\rangle, \tag{4.102}$$

where $\{|b_i\rangle\}$ are set of d normalised vectors belonging to $\mathscr{H}_B$ that might not be orthogonal. Also α_i are real numbers greater than or equal to zero that satisfy the normalisation condition $\sum_{i=0}^{d-1} \alpha_i^2 = 1$.

The proof for bounding the distance between the actual state $|\psi\rangle$ and the ideal state $|\phi_+^d\rangle$ is divided into two major parts. We first show that $\alpha_i's$ are close to $1/\sqrt{d}$. Then, we show that the real part of the terms $\langle i|b_i\rangle$ are close to 1. The proof for finding robustness of the measurements (4.98) and (4.99) is quite straightforward and follows directly from the robustness of state (4.97) using simple manipulations.

Let us first consider the inequality (4.101) for $y = 1$, and then substitute into it $A_1 = X_d Z_d^l$ and the state (4.102), which gives

$$\mathrm{Re}\left(\sum_j \alpha_j \langle j|\langle b_j|\left[\left(X_d Z_d^l\right)^k \otimes B_1^k\right]\sum_i \alpha_i |i\rangle|b_i\rangle\right) \geq 1 - \varepsilon \tag{4.103}$$

for every k. Notice that $(X_d Z_d^l)^k|i\rangle = \omega^{kl\left(i+\frac{k-1}{2}\right)}|i+k\rangle$, where the sum $i+k$ is modulo d. Thus, we have that

$$\sum_i \alpha_i \alpha_{i+k} \mathrm{Re}\left(\omega^{kl\left(i+\frac{k-1}{2}\right)}\langle b_{i+k}|B_1^k|b_i\rangle\right) \geq 1 - \varepsilon. \tag{4.104}$$

Using the fact that

$$\mathrm{Re}\left(\omega^{kl\left(i+\frac{k-1}{2}\right)}\langle b_{i+k}|B_1^k|b_i\rangle\right) \leq \left|\omega^{kl\left(i+\frac{k-1}{2}\right)}\langle b_{i+k}|B_1^k|b_i\rangle\right| \leq \left|\langle b_{i+k}|B_1^k|b_i\rangle\right| \leq 1, \tag{4.105}$$

where we used that $|b_i\rangle$ are normalised, we have finally have that

$$\sum_{i=0}^{d-1} \alpha_i \alpha_{i+k} \geq 1-\varepsilon \quad \forall k. \tag{4.106}$$

Notice that the above relation holds trivially for $k=0$ from the normalisation condition. Summing the above relation over k, we obtain

$$\sum_{i,k=0}^{d-1} \alpha_i \alpha_{i+k} = \left(\sum_{i=0}^{d-1} \alpha_i\right)^2 \geq d(1-\varepsilon), \tag{4.107}$$

which gives

$$\sum_{i=0}^{d-1} \alpha_i \geq \sqrt{d}\sqrt{1-\varepsilon}. \tag{4.108}$$

Let us now consider the following expression,

$$\begin{aligned} \sum_{i=0}^{d-1} \left(\alpha_i - \frac{1}{\sqrt{d}}\right)^2 &= \sum_{i=0}^{d-1} \alpha_i^2 - \frac{2}{\sqrt{d}} \sum_{i=0}^{d-1} \alpha_i + 1 \\ &= 2\left(1 - \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} \alpha_i\right), \end{aligned} \tag{4.109}$$

where we used the normalisation condition $\sum_i \alpha_i^2 = 1$. The right hand side of the above equation can be upper bounded using (4.108) and thus we can finally conclude that $\alpha_i's$ are close to $1/\sqrt{d}$ by a factor of $\sqrt{2\varepsilon}$, that is,

$$\begin{aligned} \sum_{i=0}^{d-1} \left(\alpha_i - \frac{1}{\sqrt{d}}\right)^2 &\leq 2(1-\sqrt{1-\varepsilon}) \\ &\leq 2\varepsilon, \end{aligned} \tag{4.110}$$

where we used the fact that $\sqrt{1-\varepsilon} \geq 1-\varepsilon$ for any $0 \leq \varepsilon \leq 1$ and thus,

$$\frac{1}{\sqrt{d}} - \sqrt{2\varepsilon} \leq \alpha_i \leq \frac{1}{\sqrt{d}} + \sqrt{2\varepsilon}. \tag{4.111}$$

Considering the expression $\sum_{i=0}^{d-1} \left(\alpha_i \alpha_j - \frac{1}{\sqrt{d}}\right)^2$ for any $i,j = 0,\ldots,d-1$, in a similar manner as done above we can conclude that

$$\frac{1}{d} - \sqrt{2\varepsilon} \leq \alpha_i \alpha_{i+j} \leq \frac{1}{d} + \sqrt{2\varepsilon}. \tag{4.112}$$

We now consider the condition (4.101) for $y=2$ by substituting $A_2 = Z_d$ and the state

(4.102)

$$\mathrm{Re}\left(\sum_j \alpha_j \langle j|\langle b_j| \left[Z_d^k \otimes B_2^k\right] \sum_i \alpha_i |i\rangle|b_i\rangle\right) \geq 1-\varepsilon \quad \forall k. \tag{4.113}$$

Notice that $Z_d^k|i\rangle = \omega^{ik}|i\rangle$ and thus the above equation simplifies to

$$\sum_{i=0}^{d-1} \alpha_i^2 \,\mathrm{Re}\left(\omega^{ik}\langle b_i|B_2^k|b_i\rangle\right) \geq 1-\varepsilon. \tag{4.114}$$

Again, using the property that

$$\mathrm{Re}(\omega^{ik}\langle b_i|B_2^k|b_i\rangle) \leq |\omega^{ik}\langle b_i|B_2^k|b_i\rangle| \leq |\langle b_i|B_2^k|b_i\rangle| \leq 1 \tag{4.115}$$

for every i,k as $|b_i\rangle$ is normalised. Thus, we can choose an index j such that

$$\sum_{i\neq j} \alpha_i^2 + \alpha_j^2 \,\mathrm{Re}\left(\omega^{jk}\langle b_j|B_2^k|b_j\rangle\right) \geq 1-\varepsilon. \tag{4.116}$$

Using the normalisation condition $\sum_i \alpha_i^2 = 1$, we arrive at

$$\alpha_j^2 \left[1-\mathrm{Re}\left(\omega^{jk}\langle b_j|B_2^k|b_j\rangle\right)\right] \leq \varepsilon. \tag{4.117}$$

Again using the property (4.112),and then the inequality (4.111), we arrive at

$$\begin{aligned} \frac{1}{d}\left[1-\mathrm{Re}\left(\omega^{jk}\langle b_j|B_2^k|b_j\rangle\right)\right] &\leq \varepsilon + \sqrt{2\varepsilon}\left[1-\mathrm{Re}\left(\omega^{jk}\langle b_j|B_2^k|b_j\rangle\right)\right] \\ &\leq \varepsilon + 2\sqrt{2\varepsilon} \\ &\leq 3\sqrt{2\varepsilon}, \end{aligned} \tag{4.118}$$

where we used the fact that the maximum of the term $\left[1-\mathrm{Re}\left(\omega^{jk}\langle b_j|B_2^k|b_j\rangle\right)\right]$ is two. Thus, we can finally conclude that

$$\mathrm{Re}\left(\omega^{jk}\langle b_j|B_2^k|b_j\rangle\right) \geq 1-3d\sqrt{2\varepsilon}. \tag{4.119}$$

Recall that the eigenvalues of B_2 is $\{1,\omega,\ldots,\omega^{d-1}\}$ and thus we can consider the eigen-decomposition of B_2 using orthogonal projections P_i as

$$B_2 = \sum_{i=0}^{d-1} \omega^i P_i. \tag{4.120}$$

Here P_i in general might be of rank higher than one. Plugging this decomposition into

the condition (4.119), we have that

$$\sum_{i=0}^{d-1} \mathrm{Re}\left(\omega^{(i+j)k}\langle b_j|P_i|b_j\rangle\right) \geq 1-3d\sqrt{2\varepsilon} \quad \forall k. \tag{4.121}$$

Notice that the above equation holds trivially for $k=0$. Taking a sum over k gives us

$$\langle b_j|P_{-j}|b_j\rangle \geq 1-3d\sqrt{2\varepsilon}, \tag{4.122}$$

which implies that each vector $|b_j\rangle$ is close to the projection P_{-j} which signifies the subspace corresponding to the $(d-j)-th$ outcome of B_2. Now, let us look at the following normalised vectors

$$|\bar{v}_j\rangle = \frac{P_{-j}|b_j\rangle}{\|P_{-j}|b_j\rangle\|}, \tag{4.123}$$

where we can infer that $|\bar{v}_j\rangle$ are mutually orthogonal as well, that is, $\langle\bar{v}_i|\bar{v}_j\rangle = \delta_{i,j}$. Note that, from the condition (4.122) the normalisation factor of each of the vector $|\bar{v}_j\rangle$ is close to one, that is, $\|P_{-j}|b_j\rangle\| \geq 1-2d\sqrt{2\varepsilon}$. Further, using these vectors we can express B_2 as

$$B_2 = \sum_{i=0}^{d-1} \omega^{-i}|\bar{v}_i\rangle\langle\bar{v}_i| \oplus B_2', \tag{4.124}$$

such that B_2' is some operator acting on the support orthogonal to the subspace spanned by the vectors $\{|\bar{v}_i\rangle\}$. Now, there always exist a unitary $U_B : \mathscr{H}_B \to \mathscr{H}_B$ such that $U_B|\bar{v}_i\rangle = |i\rangle$ and thus,

$$U_B B_2 U_B^\dagger = \sum_{i=0}^{d-1} \omega^{-i}|i\rangle\langle i| \oplus B_2''. \tag{4.125}$$

Substituting the above form of B_2 to (4.119) and then taking a sum over k, we can also deduce that

$$\mathrm{Re}\left(\langle b_i|U_B^\dagger|i\rangle\right) \geq 1-3d\sqrt{2\varepsilon}. \tag{4.126}$$

Finally, we can compute the distance between the states (4.97) using the above results as,

$$\begin{aligned} \left\|\mathbb{1}_A \otimes U_B|\psi\rangle - |\phi_d^+\rangle\right\| &= \left\{2\left[1-\mathrm{Re}(\langle\psi|U_B^\dagger|\phi_d^+\rangle)\right]\right\}^{1/2} \\ &= \left\{2\left[1-\frac{1}{\sqrt{d}}\sum_i \alpha_i \mathrm{Re}(\langle b_i|U_B^\dagger|i\rangle)\right]\right\}^{1/2}. \end{aligned} \tag{4.127}$$

Now, using the conditions (4.108) and (4.126), we have

$$\begin{aligned}\sum_i \alpha_i \mathrm{Re}(\langle b_i|U_B^\dagger|i\rangle) &\geq (1-3d\sqrt{2\varepsilon})\sum_i \alpha_i \\ &\geq (1-3d\sqrt{2\varepsilon})\sqrt{d}\sqrt{1-\varepsilon} \\ &\geq \sqrt{d}\left[1-(3d+1)\sqrt{2\varepsilon}\right], \end{aligned} \tag{4.128}$$

where the inequality in the third line is a consequence of two inequalities, first, $\sqrt{1-\varepsilon} \geq 1-\varepsilon$ for any $\varepsilon \leq 1$ and second, $\varepsilon \leq \sqrt{2\varepsilon}$. Using the inequality (4.128), we finally obtain the robustness of the state (4.97) as

$$\left\|(\mathbb{1}_A \otimes U_B)\,|\psi\rangle - |\phi_d^+\rangle\right\| \leq \sqrt{2(3d+1)}\sqrt[4]{2\varepsilon}. \tag{4.129}$$

Let us now prove the inequalities (4.98) and (4.99). For simplicity, we denote the ideal observables as B_i' and $U_B B_i U_B^\dagger = \widetilde{B}_i$. We first observe that the Hilbert Schmidt norm can be written as a vector norm using $|\phi_+^d\rangle$ as

$$\left\|\widetilde{B}_i^k - (B_i')^k\right\|_2 = \sqrt{d}\left\|\left[\widetilde{B}_i^k - (B_i')^k\right]|\phi_d^+\rangle\right\|. \tag{4.130}$$

Then, using the triangle inequality $|A+B| \geq ||A|-|B||$ and denoting $|\widetilde{\psi}\rangle = \mathbb{1}_A \otimes U_B|\psi\rangle$, we have that

$$\begin{aligned}\left\|\widetilde{B}_i^k|\widetilde{\psi}\rangle - (B_i')^k|\phi_d^+\rangle\right\| &= \left\|\widetilde{B}_i^k|\widetilde{\psi}\rangle - (B_i')^k|\phi_d^+\rangle + (B_i')^k|\phi_d^+\rangle - \widetilde{B}_i^k|\phi_d^+\rangle\right\| \\ &\geq \left\|\left[\widetilde{B}_i^k - (B_i')^k\right]|\phi_d^+\rangle\right\| - \left\|\widetilde{B}_i^k(|\widetilde{\psi}\rangle - |\phi_d^+\rangle)\right\|, \end{aligned} \tag{4.131}$$

Then using using the inequality (4.130) and the fact that B_i is unitary, leads us to

$$\left\|\widetilde{B}_i^k - (B_i')^k\right\|_2 \leq \sqrt{d}\left(\left\|\widetilde{B}_i^k|\widetilde{\psi}\rangle - (B_i')^k|\phi_d^+\rangle\right\| + \left\||\widetilde{\psi}\rangle - |\phi_d^+\rangle\right\|\right). \tag{4.132}$$

The first term in the right hand side of the above inequality can be computed using (4.127) by first noting that $A_i^k \otimes B_i'^k|\phi_+^d\rangle = |\phi_+^d\rangle$ and then using the fact that A_i is unitary,

$$\left\|(A_i^k \otimes \widetilde{B}_i^k)|\widetilde{\psi}\rangle - |\widetilde{\psi}\rangle + |\widetilde{\psi}\rangle - |\phi_d^+\rangle\right\| \leq \left\|(A_i^k \otimes \widetilde{B}_i^k)|\widetilde{\psi}\rangle - |\widetilde{\psi}\rangle\right\| + \left\||\widetilde{\psi}\rangle - |\phi_d^+\rangle\right\|. \tag{4.133}$$

Finally using the conditions (4.101) we get

$$\begin{aligned}\left\|(A_i^k\otimes\widetilde{B}_i^k)|\widetilde{\psi}\rangle-|\widetilde{\psi}\rangle\right\| &= \left\|(A_i^k\otimes B_i^k)|\psi\rangle-|\psi\rangle\right\| \\ &= \left\{2\left[1-\mathrm{Re}\left(\langle\psi|A_i^k\otimes B_i^k|\psi\rangle\right)\right]\right\}^{1/2} \\ &\leq \sqrt{2\varepsilon}. \end{aligned} \tag{4.134}$$

Using the above inequality, we get that

$$\left\|(A_i^k\otimes\widetilde{B}_i^k)|\widetilde{\psi}\rangle-|\widetilde{\psi}\rangle+|\widetilde{\psi}\rangle-|\phi_d^+\rangle\right\| \leq \sqrt{2\varepsilon}+2\left\||\widetilde{\psi}\rangle-|\phi_d^+\rangle\right\|, \tag{4.135}$$

and then using the condition (4.97) we obtain (4.98) and (4.99). □

4.5 Conclusions and discussions

We proposed a one-sided device-independent scheme for a certification of a large family of incompatible measurements with arbitrary number of outcomes termed here genuinely incompatible. Our scheme also allows for the certification of the two-qudit maximally entangled of any arbitrary local dimension using only two measurements on each side. This is the first certification of mutually unbiased bases of any dimension using quantum steering. Unlike the previous approaches in literature, our scheme is more general in the sense that we do not assume that the state shared between the parties is pure or the measurements on the untrusted side are projective. This makes our scheme even significant in cryptographic scenarios where there can be an external Eve who can have access to the state as well as the untrusted measurements. We also find a simple technique for robust certification of a smaller family of genuinely incompatible observables including the complete mutually unbiased bases of any prime dimension and pair of them for non-prime dimensions. We also considered the scenario when the measurements are not genuinely incompatible and observed that only a part of the measurement can be certified based on the quantum state that realises the quantum bound of the steering functional.

One of the drawbacks of the 1SDI scheme as compared to fully device-independent schemes is that one has to assume that one of the parties is trusted. However, they still posses some of the essential features that would be useful in certification of quantum technologies. First, if one possesses a well characterised quantum device, here it is the measuring device of the trusted party, our scheme provides a way to compare any other untrusted device with the trusted device using minimal resources. In other words, our scheme given a trusted measurement device allows one to verify that any other device performs the desired measurements. Second, our scheme is applicable to every 1SDI scenario

where a client wants to verify the state supplied by an untrusted source along with the untrusted measuring device. Thus, one-sided quantum key distribution schemes [111], [112] and randomness generation would be two major applications of our certification scheme. Third, even from a practical point of view, implementing 1SDI protocols is much easier than the DI protocols [111]. The reason being that demonstration of quantum steering is practically more robust to noise and can be observed with detectors of lower efficiencies than Bell violations [164], [165]. Fourth, there are a very few analytical methods dedicated to the field of quantum certification, let alone to higher dimensional quantum certification. Thus, purely from a mathematical perspective, we introduced techniques that can be relevant for other schemes that aim to characterise arbitrary dimensional quantum systems. Finally, in certain scenarios 1SDI schemes can be made device-independent if one can device-independently characterise the measuring device of the trusted party as pointed out recently in Ref. [62].

Some interesting follow-up problems arise from our work. The most important among them would be whether our 1SDI scheme can be made fully device-independent, that is, the question whether it is possible to design a scheme for certifying every set of genuinely incompatible observables in a device-independent way still remains open. Another interesting problem would be to find 1SDI scheme that can be used for certification of incompatible observables that are not genuine incompatible. It would also be interesting to construct steering functionals whose quantum bound is saturated by non-maximally entangled state of arbitrary local dimension d and thus eventually finding a scheme allowing for certification of every bipartite entangled state. This problem is tackled in the next chapter of this thesis. An ambitious problem would be extend the idea of genuine incompatibility to non-projective schemes and then find steering functionals for certification of POVM's.

Chapter 5

Certification of any pure bipartite entangled state and optimal randomness using quantum steering

5.1 Introduction

Generating genuine random outputs inaccessible to hackers is one of the key steps in any key distribution protocol, be it classical or quantum. As discussed before in Chapter 2, in classical physics the security of such protocols relies on the fact that large numbers can not be efficiently factorized using classical computers. However, using quantum computers such protocols can be broken in polynomial time. As was shown in [65], violation of Bell inequalities serve as the most secure way to certify genuine randomness. However, from a practical point of view, performing a Bell experiment is extremely challenging as one requires very low levels of noise along with the detectors being highly efficient. As a consequence, we need to consider scenarios where one can efficiently generate secure randomness, easier to implement, require minimal resources and are robust to noise. We showed in Chapter 3 that one can securely generate $\log_2 d$ bits of randomness using a quantum system of dimension d. From a foundational point of view, it still remains an open and highly non-trivial problem whether one can securely generate the optimal amount of randomness using a quantum system of arbitrary dimension d which is $2\log_2 d$ bits.

In this chapter, we aim to solve the above problem by considering the one-sided device-independent (1SDI) scenario where the required resource is quantum steering. As a matter of fact, it was shown in [111] that quantum steering can be observed using detectors with much lower efficiency and more noise-robust when compared to observing Bell non-

locality. This makes 1SDI setting an ideal scenario to construct protocols for randomness generation that can be practically implemented. Randomness generation in 1SDI setting has been recently explored in [122], [166]. Particularly in Ref. [166], the authors construct a protocol for generating $\log_2 d$ bits of randomness from a quantum system of dimension d in a secure way by using d-outcome projective measurements.

To this end, we first construct a family of steering inequalities maximally violated by any pure entangled state of local dimension d and two $d-$outcome measurements on each side. Using the maximal violation of the steering inequalities, we then certify any pure bipartite entangled state and a pair of mutually unbiased bases of arbitrary dimension on the untrusted side. This is the first instance, where any pure bipartite entangled state can be certified using the least number of measurements required to observe quantum non-locality, that is, using only two measurements on each side. Additionally, we demonstrate that any rank-one extremal measurement can be certified using our protocol. Based on these results, we finally demonstrate the certification of $2\log_2 d$ bits of randomness using the certified entangled state of local dimension d and the certified d^2-outcome extremal measurement. We further show that for systems of dimension $d = 3,4,5,6$, the optimal amount of randomness can be certified using partially entangled states. This further strengthens our scheme as one can generate highest amount of randomness by employing less resource in terms of entanglement.

5.2 Family of steering inequalities

Let us shortly describe again the quantum steering scenario introduced in Chapter 2 and also in Chapter 4 in an analogous way to Bell scenario. Alice and Bob are located in spatially separated labs. Both of them receive two subsystems from a preparation device. Alice is trusted and performs two known $d-$outcome measurements on the received subsystem labelled by $x = 1,2$. In our case, we consider these measurements in the observable form as $A_0 = Z_d$ and $A_1 = X_d$ which as described in Eq. (2.91) of Chapter 4, constitute a pair of mutually unbiased bases. Bob also performs two $d-$outcome measurements on his subsystem labelled by $y = 1,2$. They collect enough statistics to construct the joint probability distribution $\{p(a,b|x,y)\}$. The scenario is depicted in Fig. 4.1 of Chapter 4 such that $N = 2$.

We now construct a family of steering inequalities which is expressed in the observable picture and using a collection of positive non-zero numbers $\boldsymbol{\alpha} = \{\alpha_0, \alpha_1, \ldots, \alpha_{d-1}\}$ such that $\sum_{i=0}^{d-1} \alpha_i^2 = 1$, as

$$I_{2,d,2}(\boldsymbol{\alpha}) = \sum_{k=1}^{d-1} \left\langle A_0^k \otimes B_{k|0} + \gamma(\boldsymbol{\alpha}) A_1^k \otimes B_{k|1} + \delta_k(\boldsymbol{\alpha}) A_0^k \right\rangle \leq \beta_L(\boldsymbol{\alpha}), \tag{5.1}$$

where the coefficients $\gamma(\boldsymbol{\alpha})$ and $\delta_k(\boldsymbol{\alpha})$ are given by

$$\gamma(\boldsymbol{\alpha}) = d\left(\sum_{\substack{i,j=0\\ i\neq j}}^{d-1}\frac{\alpha_i}{\alpha_j}\right)^{-1}, \qquad \delta_k(\boldsymbol{\alpha}) = -\frac{\gamma(\boldsymbol{\alpha})}{d}\sum_{\substack{i,j=0\\ i\neq j}}^{d-1}\frac{\alpha_i}{\alpha_j}\omega^{k(d-j)}. \tag{5.2}$$

Notice that $\gamma(\boldsymbol{\alpha}) \geq 0$ for any choice of $\boldsymbol{\alpha}$ and $\delta_k(\boldsymbol{\alpha})$ are in general complex. Alice is trusted (or fully characterised), and her measurements are expressed in the observable picture as

$$A_0 = Z_d = \sum_{i=0}^{d-1}\omega^i|i\rangle\langle i|, \qquad A_1 = X_d = \sum_{i=0}^{d-1}|i+1\rangle\langle i|. \tag{5.3}$$

Recall that the set of vectors $\{|i\rangle\}_{i=0}^{d-1}$ represents the computational basis in $\mathbb{C}^d$. It is worth noting here that the expression $I_{2,d,2}(\boldsymbol{\alpha})$ (2.67) is real for any choice of $\boldsymbol{\alpha}$. This is because $B_{d-k|i} = (B_{k|i})^\dagger$ for any generalised observable (see Eq. (2.22) of Chapter 2) and also that the coefficient $\delta_{d-k}(\boldsymbol{\alpha}) = \delta_k^*(\boldsymbol{\alpha})$ for any k. Let us now express the steering functional in (2.67) using the joint probability picture as

$$\begin{aligned} I_{2,d,2}(\boldsymbol{\alpha}) = d\sum_{a,b=0}^{d-1}c_{a,b}p(a,b|0,0) \;&+\; \gamma(\boldsymbol{\alpha})\left(d\sum_{a,b=0}^{d-1}c_{a,b}p(a,b|1,1) - \sum_{\substack{i,a=0\\ i\neq a}}^{d-1}\alpha_i\frac{p(a|0)}{\alpha_a}\right)\\ &-\; 1-\gamma(\boldsymbol{\alpha})-\delta_0(\boldsymbol{\alpha}), \end{aligned} \tag{5.4}$$

such that

$$c(a,b) = \begin{cases} 1 & \text{if} \quad a\oplus_d b = 0\\ 0 & \text{otherwise} \end{cases}, \tag{5.5}$$

where $a\oplus_d b$ represents $a+b$ modulo d. To arrive at the above expression we used the fourier transform to express the expectation values in terms of the joint probabilities as defined in (4.4). Note from Eq. (5.2) that $\delta_0(\boldsymbol{\alpha}) = -1$, which implies that

$$I_{2,d,2}(\boldsymbol{\alpha}) = d\sum_{a,b=0}^{d-1}c_{a,b}p(a,b|0,0) + \gamma(\boldsymbol{\alpha})\left(d\sum_{a,b=0}^{d-1}c_{a,b}p(a,b|1,1) - \sum_{i=0}^{d-1}\alpha_i\sum_{a=0}^{d-1}\frac{p(a|0)}{\alpha_a}\right). \tag{5.6}$$

Using the above expression of the steering functional, let us now compute the classical bound $\beta_L(\boldsymbol{\alpha})$ of the above steering inequality.

5.2.1 Classical bound

As derived before in Eq. (4.7) of Chapter 4, to find the classical bound of a steering functional, we need to consider an LHS model such that the joint probability distribution can be expressed as

$$p(a,b|x,y) = \sum_{\lambda} p(\lambda)p(a|x,\rho_\lambda)p(b|y,\lambda), \tag{5.7}$$

where λ denotes some unknown variables the collection of which is denoted by $\boldsymbol{\lambda}$. These variables occur with a probability distribution $p(\lambda)$. Here $p(a|x,\rho_\lambda)$ is the local probability of Alice obtaining an outcome a given the input x and some quantum state ρ_λ acts on $\mathbb{C}^d$ [1] and $p(b|y,\lambda)$ is the local probability distribution depending on some unknown variable λ. For such a probability distribution (5.7), the steering functional from Eq. (5.6) can be expressed as,

$$\begin{aligned} I_{2,d,2}(\boldsymbol{\alpha}) &= d\sum_{a=0}^{d-1}\sum_{\lambda} p(\lambda)p(a|0,\rho_\lambda)p(d-a|0,\lambda) \\ &+ \gamma(\boldsymbol{\alpha})\left(d\sum_{a=0}^{d-1}\sum_{\lambda} p(\lambda)p(a|1,\rho_\lambda)p(d-a|1,\lambda) - \sum_i \alpha_i \sum_{a=0}^{d-1}\sum_{\lambda}\frac{p(\lambda)p(a|0,\rho_\lambda)}{\alpha_a}\right), \end{aligned} \tag{5.8}$$

where to obtain the last term, we used the no-signalling conditions given in Eq. (2.53) of Chapter 2 such that

$$p(a|0) = \sum_b p(a,b|0,y) \qquad \forall y. \tag{5.9}$$

Notice that in the above expression we used the fact that $\sum_b p(b|y,\lambda) = 1$ for any λ and then denoted $\rho_A = \sum_\lambda p(\lambda)\rho_\lambda$. Let us first consider the first two terms in Eq. (5.8) and find their upper bound in the following way,

$$\begin{aligned} I_{2,d,2}(\boldsymbol{\alpha}) &\leq d\sum_{a=0}^{d-1}\sum_{\lambda} p(\lambda)\max_a p(a|0,\rho_\lambda) \\ &+ \gamma(\boldsymbol{\alpha})\left(d\sum_{a=0}^{d-1}\sum_{\lambda} p(\lambda)\max_a p(a|1,\rho_\lambda) - \sum_i \alpha_i \sum_{a=0}^{d-1}\sum_{\lambda}\frac{p(\lambda)p(a|0,\rho_\lambda)}{\alpha_a}\right), \end{aligned} \tag{5.10}$$

where $y = 0,1$ and to obtain the first inequality we used the fact that $\sum_a p(d-a|y,\lambda) = 1$

[1] This is due to the fact that Alice is trusted and is known to perform quantum measurments on some quantum state.

for any y and λ and then used the mathematical identity $\sum_i s_i w_i \leq \max_i\{s_i\}$ whenever $w_i \geq 0$ and $\sum_i w_i = 1$. Now as was done before in Chapter 4 [see Eq. (4.12)] and using the fact that $\sum_\lambda p(\lambda) = 1$, we get that

$$I_{2,d,2}(\boldsymbol{\alpha}) \leq \max_{\rho} \left[d \max_a \{p(a|0,\rho)\} + \gamma(\boldsymbol{\alpha}) \left(d \max_a \{p(a|1,\rho)\} - \sum_{i=0}^{d-1} \alpha_i \sum_{a=0}^{d-1} \frac{p(a|0,\rho)}{\alpha_a} \right) \right]. \tag{5.11}$$

Notice the above expression is convex in the state ρ. As a consequence, the maximisation in the above expression can be taken over pure states $|\psi\rangle \in \mathbb{C}^d$. Now expressing the state $|\psi\rangle$ in the computational basis of $\mathbb{C}^d$ as $|\psi\rangle = \sum_i \eta_i |i\rangle$, and then plugging in Alice's observables, $A_0 = Z_d$ and $A_1 = X_d$, the formula (5.11) can be rewritten as

$$I_{2,d,2}(\boldsymbol{\alpha}) \leq \max_{\substack{|\eta_0|,\ldots,|\eta_{d-1}| \\ |\eta_0|^2+\ldots+|\eta_{d-1}|^2=1}} \left\{ d \max_a \{|\eta_a|^2\} + \gamma(\boldsymbol{\alpha}) \left[\left(\sum_{i=0}^{d-1} |\eta_i| \right)^2 - \sum_{i=0}^{d-1} \alpha_i \sum_{a=0}^{d-1} \frac{|\eta_a|^2}{\alpha_a} \right] \right\}. \tag{5.12}$$

Given any arbitrary collection of positive numbers $\boldsymbol{\alpha}$ such that the sum of the squares of those numbers is one, it is not straightforward to find this bound. However, we can show here that the right hand side of the above formula is strictly less than d for any $\boldsymbol{\alpha}$. We prove this claim using the technique of contradiction. Let us first consider the term inside the square brackets of the above expression (5.12) and show that it is always negative. For this, let us recall the Cauchy–Schwarz inequality for positive real numbers also known as Sedrakyan's inequality [167],

$$\frac{(\sum_i u_i)^2}{\sum_i v_i} \leq \sum_i \frac{u_i^2}{v_i}. \tag{5.13}$$

Now, substituting $u_i = |\eta_i|$ and $v_i = \alpha_i$, we can rewrite the above expression as

$$\left(\sum_{i=0}^{d-1} |\eta_i| \right)^2 \leq \sum_{i=0}^{d-1} \alpha_i \sum_{j=0}^{d-1} \frac{|\eta_i|^2}{\alpha_i}. \tag{5.14}$$

Thus, we can conclude from (5.12) that the the classical bound of $I_{2,d,2}(\boldsymbol{\alpha})$ is less than or equal to d, that is,

$$I_{2,d,2}(\boldsymbol{\alpha}) \leq d \max_a \{|\eta_a|^2\} \leq d. \tag{5.15}$$

We now show that the above inequlity can not be saturated by L.H.S. models. To this end, let us assume that $I_{2,d,2}(\boldsymbol{\alpha}) = d$. This implies that the term inside the square brackets

in (5.12) vanishes and thus,

$$\left(\sum_{i=0}^{d-1}|\eta_i|\right)^2=\sum_{i=0}^{d-1}\alpha_i\sum_{j=0}^{d-1}\frac{|\eta_i|^2}{\alpha_i}. \tag{5.16}$$

along with the first term

$$\max_a\{|\eta_a|^2\}=1. \tag{5.17}$$

Recall that equality holds in the Cauchy–Schwarz inequality (5.13) iff $u_i=\kappa v_i$ for all i where κ is some real coefficient. Thus, in (5.16) $\alpha_i=\kappa|\eta_i|$ for each i. Using the condition $\sum_i\alpha_i^2=\sum_i|\eta_i|^2=1$ and that $\alpha_i>0$ for any i, imposes that $\kappa=1$, and therefore $\alpha_i=|\eta_i|$. But $\alpha_i<1$ for any i which contradicts the second condition (5.17). Thus, our initial assumption is wrong which implies that the maximal classical value of the steering function $I_{2,d,2}(\boldsymbol{\alpha})$ is strictly less than d for arbitrary collection of positive numbers α_i such that $\alpha_0^2+\ldots+\alpha_{d-1}^2=1$. Now, we move onto finding the quantum bound of the steering functional in (2.67).

5.2.2 Quantum bound

Here we show that the maximum value of the steering functional $I_{2,d,2}(\boldsymbol{\alpha})$ in Eq. (5.1) obtainable using quantum states and measurements is given by $\beta_Q(\boldsymbol{\alpha})=d$. The result is stated below as a mathematical theorem.

Theorem 5.1. *For any collection of positive real numbers* $\boldsymbol{\alpha}=\{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}\}$ *such that* $\alpha_0^2+\ldots+\alpha_{d-1}^2=1$, *the quantum bound of the steering functional* $I_{2,d,2}(\boldsymbol{\alpha})$ *is independent of* $\boldsymbol{\alpha}$ *and is given by* $\beta_Q(\boldsymbol{\alpha})=d$.

Proof. Let us begin by introducing the steering operator corresponding to the steering functional $I_{2,d,2}(\boldsymbol{\alpha})$ in (5.1),

$$\hat{I}_{2,d,2}(\boldsymbol{\alpha})=\sum_{k=1}^{d-1}\left(A_0^k\otimes B_{k|0}+\gamma(\boldsymbol{\alpha})A_1^k\otimes B_{k|1}+\delta_k(\boldsymbol{\alpha})A_0^k\right). \tag{5.18}$$

Recall that $A_0=Z_d$ and $A_1=X_d$ and $B_i's$ are any d-outcome generalised observables corresponding to the measurements of Bob. Our aim is to show that

$$\beta_Q(\boldsymbol{\alpha})=\max_{\rho_{AB},B_i}\mathrm{Tr}\left[\hat{I}_{2,d,2}(\boldsymbol{\alpha})\rho_{AB}\right]=d, \tag{5.19}$$

where ρ_{AB} acting on $\mathbb{C}^d\otimes\mathscr{H}_B$ represents some quantum state shared between Alice and Bob and $\mathscr{H}_B$ represents the Hilbert space of Bob of arbitrary but finite dimension. As the expression (5.19) is linear, we can optimise this over pure states $|\psi_{AB}\rangle\in\mathbb{C}^d\otimes\mathscr{H}_B$, that

is,

$$\max_{|\psi_{AB}\rangle, B_i} \langle \psi_{AB} | \hat{I}_{2,d,2} | \psi_{AB} \rangle = d. \tag{5.20}$$

For simplicity, in the rest of the proof we drop the subscript AB from the state. We first show that the expectation value of the steering operator for any $|\psi\rangle$ is upper bounded by d and then find a quantum realisation that achieves this bound. For this purpose, let us break the steering operator $\hat{I}_{2,d,2}(\boldsymbol{\alpha})$ into two parts as

$$\hat{I}_{2,d,2}(\boldsymbol{\alpha}) = \sum_{k=1}^{d-1} A_0^k \otimes B_{k|0} + S(\boldsymbol{\alpha}) \tag{5.21}$$

such that

$$S(\boldsymbol{\alpha}) = \sum_{k=1}^{d-1} \left[\gamma(\boldsymbol{\alpha}) A_1^k \otimes B_{k|1} + \delta_k(\boldsymbol{\alpha}) A_0^k \right]. \tag{5.22}$$

Notice that the above operator is hermitian which is due to the fact that $A_0^{d-k} = (A_0^k)^\dagger$ and $B_{d-k|0} = B_{k|0}^\dagger$ [see Eq. (2.22)]. It is trivial to see that the absolute values of the expectation value of each term in the first part of operator in Eq. (5.21) is less than or equal to 1 as A_0 is unitary and $B_{k|0}^\dagger B_{k|0} \leq \mathbb{1}$ for any k [see Eq. (2.23)], that is,

$$|\langle \psi | A_0^k \otimes B_{k|0} | \psi \rangle| \leq 1, \tag{5.23}$$

for any $|\psi\rangle$ and $k = 1, \ldots, d-1$. This allows us to conclude from (5.21) that

$$\langle \psi | \hat{I}_{2,d,2}(\boldsymbol{\alpha}) | \psi \rangle \;\; \leq \;\; d - 1 + \langle \psi | S(\boldsymbol{\alpha}) | \psi \rangle. \tag{5.24}$$

Now, we demonstrate for any $|\psi\rangle$ that $\langle \psi | S(\boldsymbol{\alpha}) | \psi \rangle \leq 1$. For this purpose, let us first notice that the state $|\psi\rangle$ belongs to $\mathbb{C}^d \otimes \mathscr{H}_B$. Thus, as discussed before in Chapter 2 any such state can be written using the computational basis in $\mathbb{C}^d$ as

$$|\psi_{ABE}\rangle = \sum_{i=0}^{d-1} \lambda_i |i\rangle_A |e_i\rangle_B, \tag{5.25}$$

where λ_i are real and non-negative numbers such that $\lambda_0^2 + \ldots + \lambda_{d-1}^2 = 1$, and $|e_i\rangle$ are vectors belonging to $\mathscr{H}_B$ which are not orthogonal in general. Plugging in this state, we find the expectation value of $S(\boldsymbol{\alpha})$ as

$$\begin{aligned} \langle \psi | S(\boldsymbol{\alpha}) | \psi \rangle &= \sum_{k=1}^{d-1} \sum_{i,j=0}^{d-1} \left[\gamma(\boldsymbol{\alpha}) \lambda_i \lambda_j \langle i | A_1^k | j \rangle \langle e_i | B_{k|1} | e_j \rangle + \delta_k(\boldsymbol{\alpha}) \lambda_i \lambda_j \langle i | A_0^k | j \rangle \langle e_i | e_j \rangle \right] \\ &= \sum_{k=1}^{d-1} \sum_{i=0}^{d-1} \left[\gamma(\boldsymbol{\alpha}) \lambda_i \lambda_{i-k} \langle e_i | B_{k|1} | e_{i-k} \rangle + \delta_k(\boldsymbol{\alpha}) \lambda_i^2 \omega^{ik} \right], \end{aligned} \tag{5.26}$$

where to arrive at the second equality, we plugged in the explicit forms of $A_i's$ and then used the fact that $Z_d^k|i\rangle = \omega^{ki}|i\rangle$ and $X_d^k|i\rangle = |i+k\rangle$. Focusing on the second term of the above expression and plugging in $\delta_0(\boldsymbol{\alpha}) = -1$, we obtain that

$$\sum_{k=1}^{d-1}\sum_{i=0}^{d-1}\delta_k(\boldsymbol{\alpha})\lambda_i^2\omega^{ik} = 1 + \sum_{k=0}^{d-1}\sum_{i=0}^{d-1}\delta_k(\boldsymbol{\alpha})\lambda_i^2\omega^{ik}. \tag{5.27}$$

Using then the explicit form of $\delta_k(\boldsymbol{\alpha})$ given in Eq. (5.2), we arrive at

$$\sum_{k=1}^{d-1}\sum_{i=0}^{d-1}\delta_k(\boldsymbol{\alpha})\lambda_i^2\omega^{ik} = 1 + \gamma(\boldsymbol{\alpha}) - \gamma(\boldsymbol{\alpha})\sum_{i,j=0}^{d-1}\frac{\alpha_i}{\alpha_j}\lambda_j^2, \tag{5.28}$$

where we also used the identity

$$\sum_{k=0}^{d-1}\omega^{k(i-j)} = d\delta_{ij}. \tag{5.29}$$

Notice that since $\gamma(\boldsymbol{\alpha})$ is real, the above expression (5.28) is also real. Since, $S(\boldsymbol{\alpha})$ is a Hermitian operator we have that any expectation value of this operator is real. Plugging the relations (5.28) and remembering that $\lambda_i's$ are also real, we can rewrite Eq. (5.26) as

$$\langle\psi|S(\boldsymbol{\alpha})|\psi\rangle = 1 + \gamma(\boldsymbol{\alpha})\sum_{k=0}^{d-1}\sum_{i=0}^{d-1}\lambda_i\lambda_{i-k}\mathrm{Re}\left(\langle e_i|B_{k|1}|e_{i-k}\rangle\right) - \gamma(\boldsymbol{\alpha})\sum_{i,j=0}^{d-1}\frac{\alpha_i}{\alpha_j}\lambda_j^2. \tag{5.30}$$

Exploiting the fact that $\mathrm{Re}(z) \leq |z|$ for any $z \in \mathbb{C}$ and that $B_{k|1}^\dagger B_{k|1} \leq \mathbb{1}$ for any k, we get that $\mathrm{Re}\left(\langle e_i|B_{k|1}|e_{i-k}\rangle\right) \leq 1$, Thus, we finally arrive at

$$\langle\psi|S(\boldsymbol{\alpha})|\psi\rangle \leq 1 + \gamma(\boldsymbol{\alpha})\left[\left(\sum_{i=0}^{d-1}\lambda_i\right)^2 - \sum_{i=0}^{d-1}\alpha_i\sum_{j=0}^{d-1}\frac{\lambda_j^2}{\alpha_j}\right]. \tag{5.31}$$

Now, using the Cauchy-Schwarz inequality (5.13) in which we substitute $u_i = \lambda_i$ and $v_i = \alpha_i$, we can conclude that the term inside the square brackets of the above expression is less than or equal to 0. Thus, we can finally conclude that the expectation value of $S(\boldsymbol{\alpha})$ for any state $|\psi\rangle$ is less than or equal to 1. that is,

$$\langle\psi|S(\boldsymbol{\alpha})|\psi\rangle \leq 1 \tag{5.32}$$

and hence, putting it back into (5.24), we obtain

$$\langle\psi|\hat{I}_{2,d,2}(\boldsymbol{\alpha})|\psi\rangle \leq d, \tag{5.33}$$

for any $|\psi\rangle \in \mathbb{C}^d \otimes \mathscr{H}_B$. It is also interesting to note here that the relation (5.32) is saturated when

$$\left(\sum_{i=0}^{d-1} \lambda_i\right)^2 = \sum_{i=0}^{d-1} \alpha_i \sum_{j=0}^{d-1} \frac{\lambda_j^2}{\alpha_j}. \tag{5.34}$$

Now, using the fact that Sedrakyan's inequality (5.13) is saturated if $u_i = \kappa v_i$ for some $\kappa \in \mathbb{C}$. Substituting $u_i = \lambda_i$ and $v_i = \alpha_i$ in the Sedrakyan's inequality (5.13), we see that $\lambda_i = \kappa \alpha_i$ for all i. Now, using normalisation we get that the only solution of Eq. (5.34) is $\lambda_i = e^{i\phi}\alpha_i$ for some arbitrary phase ϕ. As $\alpha_i > 0$, we get that $|\lambda_i| > 0$ for all i. Thus, we can simply conclude that any state saturating the inequality (5.32) is locally full-rank.

Let us now consider a family of states parametrized by the collection of positive real coefficients $\boldsymbol{\alpha}$,

$$|\psi(\boldsymbol{\alpha})\rangle_{AB} = \sum_{i=0}^{d-1} \alpha_i |i\rangle_A |i\rangle_B, \tag{5.35}$$

where the local bases of (5.35) is the computational basis of $\mathbb{C}^d$. Notice that the above state is a valid normalised quantum state $\sum_{i=0}^{d-1} \alpha_i^2 = 1$. Notice also that every pure bipartite entangled state of Schmidt rank d can be expressed as these states (5.35) up to local unitary transformations. Now, consider Bob's observables to be projective and to satisfy

$$B_0 = Z_d^*, \qquad B_1 = X_d. \tag{5.36}$$

Plugging this state and the observables in the steering functional in (5.1), we get that $I_{2,d,2}(\boldsymbol{\alpha}) = d$. This completes the proof. □

Notice that the maximal violation of the steering inequality (5.1) by a state $|\psi_{AB}\rangle$ and Bob's observables B_i can only be achieved iff the inequalities (5.40) and (5.43) are saturated. Thus, we arrive at the following conditions

$$\langle\psi|A_0^k \otimes B_{k|0}|\psi\rangle = 1 \tag{5.37}$$

for any $k = 1, \ldots, d-1$ as well as

$$\langle\psi|S(\boldsymbol{\alpha})|\psi\rangle = 1, \tag{5.38}$$

where $S(\boldsymbol{\alpha})$ is defined in Eq. (5.22). Now, consider the Cauchy-Schwarz inequality for

vectors given as

$$\mathrm{Re}(\langle u|v\rangle) \leq |\langle u|v\rangle| \leq |\langle u|u\rangle\langle v|v\rangle|. \tag{5.39}$$

From the condition (5.37), let us now substitute $|u\rangle = |\psi\rangle$ and $|v\rangle = A_0^k \otimes B_{k|0}|\psi\rangle$ in the above inequality (5.39). Then using the fact that $B_{k|0}^\dagger B_{k|0} \leq \mathbb{1}$, we get that both the L.H.S. and R.H.S. of (5.13) are equal to one. This can only happen iff $|u\rangle$ and $|v\rangle$ are linearly dependent, that is, $|u\rangle = \lambda|v\rangle$ for some $\lambda \in \mathbb{C}$. As both $|u\rangle$ and $|v\rangle$ are normalised, we get that $|u\rangle = e^{i\phi}|v\rangle$ where ϕ is some arbitrary phase. Putting it back into Eq. (5.37), we get that $\phi = 0$. As a consequence, we obtain the following relation

$$A_0^k \otimes B_{k|0}|\psi_{AB}\rangle = |\psi_{AB}\rangle \qquad (k = 1, \ldots, d-1). \tag{5.40}$$

Let us now consider the condition (5.38) and express $S(\boldsymbol{\alpha})$ as $S(\boldsymbol{\alpha}) = S(\boldsymbol{\alpha})_+ - S(\boldsymbol{\alpha})_-$ where $S(\boldsymbol{\alpha})_+$ is a positive matrix spanned by the eigenvectors corresponding to the positive eigenvalues of $S(\boldsymbol{\alpha})$ and $S(\boldsymbol{\alpha})_-$ is a positive matrix spanned by the eigenvectors corresponding to the negative eigenvalues of $S(\boldsymbol{\alpha})$. Plugging this decomposition in (5.38), we get that

$$\langle\psi|S(\boldsymbol{\alpha})_+|\psi\rangle = 1 + \langle\psi|S(\boldsymbol{\alpha})_-|\psi\rangle \tag{5.41}$$

Notice now from Eq. (5.32) that the maximum eigenvalue of $S(\boldsymbol{\alpha})$ is one and as a consequence $\langle\psi|S(\boldsymbol{\alpha})_+|\psi\rangle \leq 1$ and also $\langle\psi|S(\boldsymbol{\alpha})_+^2|\psi\rangle \leq 1$. Thus, from the above condition (5.41), we can conclude that $\langle\psi|S(\boldsymbol{\alpha})_-|\psi\rangle = 0$ which implies that $S(\boldsymbol{\alpha})_-|\psi\rangle = 0$ as $S(\boldsymbol{\alpha})_-$ is positive. As a consequence, we also have that $\langle\psi|S(\boldsymbol{\alpha})_+|\psi\rangle = 1$. Going back to the Cauchy-Schwarz inequality (5.39), we substitute $|u\rangle = |\psi\rangle$ and $|v\rangle = S(\boldsymbol{\alpha})|\psi\rangle$. Let us now compute $|\langle v|v\rangle|$ by using the decomposition of $S(\boldsymbol{\alpha})$ and also using the fact that it is hermitian

$$\begin{aligned}\langle\psi|S(\boldsymbol{\alpha})|\psi\rangle \leq \langle\psi|S(\boldsymbol{\alpha})^2|\psi\rangle &= \langle\psi|\left(S(\boldsymbol{\alpha})_+^2 + S(\boldsymbol{\alpha})_-^2 + S(\boldsymbol{\alpha})_+S(\boldsymbol{\alpha})_- + S(\boldsymbol{\alpha})_-S(\boldsymbol{\alpha})_+\right)|\psi\rangle \\ &= \langle\psi|S(\boldsymbol{\alpha})_+^2|\psi\rangle \leq 1 \end{aligned} \tag{5.42}$$

where to get to the second line of the above expression we used that $S(\boldsymbol{\alpha})_-|\psi\rangle = 0$. Now, as concluded before, we get that $|u\rangle = e^{i\phi}|v\rangle$ where ϕ is some arbitrary phase. Now, again using Eq. (5.38) thus we finally arrive at the relation

$$\left(\sum_{k=1}^{d-1}\left[\gamma(\boldsymbol{\alpha})A_1^k \otimes B_{k|1} + \delta_k(\boldsymbol{\alpha})A_0^k\right]\right)|\psi_{AB}\rangle = |\psi_{AB}\rangle. \tag{5.43}$$

The relations (5.40) and (5.43) would be particularly useful for certification of the quantum states and measurements that achieve the maximal violation of the steering functional $I_{2,d,2}$. Let us now show that observation of maximal violation of our steering inequalities allows us to certify the state shared between Alice and Bob and also the measurements performed by Bob.

5.3 ISDI certification of all pure bipartite entangled states

Here, we present the 1SDI certification of all pure bipartite entangled states using the saturation of the quantum bound of the steering functional (5.1) $I_{2,d,2} = \beta_Q$. Let us first recall that we can only characterise Bob's observables on the support of his local state ρ_B. Thus, without loss of generality we assume it to be full rank. This can also be understood as that Bob's observables and local state ρ_B act on the same Hilbert space $\mathscr{H}_B$.

Theorem 5.2. *Consider that Alice and Bob perform the quantum steering experiment and observe that the steering functional*

$$I_{2,d,2}(\boldsymbol{\alpha}) = \sum_{k=1}^{d-1} \left\langle A_0^k \otimes B_{k|0} + \gamma(\boldsymbol{\alpha}) A_1^k \otimes B_{k|1} + \delta_k(\boldsymbol{\alpha}) A_0^k \right\rangle, \tag{5.44}$$

attains the maximal quantum value $\beta_Q = d$ where d denotes the number of outcomes of each measurement. Alice is trusted and her measurements are given by $A_0 = Z_d$ and $A_1 = X_d$ [cf. Eq. (2.91)]. Let us say that the maximal quantum bound is achieved using the state ρ_{AB} acting on $\mathbb{C}^d \otimes \mathscr{H}_B$ and Bob's generalised observables B_i $(i \in \{1,2\})$ acting on $\mathscr{H}_B$. Then, the following statements hold true for any integer $d \geq 2$:

1. *Bob's measurements are projective. Equaivalently, the operators $B_{k|i}$ for all k, i are unitary and $B_{k|i} = B^k_{1|i} \equiv B^k_i$.*

2. *Bob's Hilbert space $\mathscr{H}_B$ admits a decomposition into a $d-$dimensional Hilbert space $\mathbb{C}^d)_{B'}$ and some unknown but finite dimensional auxiliary Hilbert space $\mathscr{H}_{B''}$,*

$$\mathscr{H}_B = (\mathbb{C}^d)_{B'} \otimes \mathscr{H}_{B''}. \tag{5.45}$$

3. *There exists a local unitary on Bob's side $U_B : \mathscr{H}_B \to \mathscr{H}_B$ such that*

$$(\mathbb{1}_A \otimes U_B)\rho_{AB}(\mathbb{1}_A \otimes U_B^\dagger) = |\psi(\boldsymbol{\alpha})\rangle\langle\psi(\boldsymbol{\alpha})|_{AB'} \otimes \rho^{aux}_{B''}. \tag{5.46}$$

where $|\psi(\boldsymbol{\alpha})\rangle$ is the state given in (5.35) and

$$\forall i, \quad U_B B_i U_B^\dagger = A_i^* \otimes \mathbb{1}_{B''}, \tag{5.47}$$

where B'' denotes Bob's auxiliary system.

Proof. The proof is divided into two major steps. In the first step, we exploit the relations (5.40) and (5.43) to find Bob's observables that result in the maximal violation of the steering inequality (5.1). Again, using the relations (5.40) and (5.43) and the derived Bob's observables, we find the family of states shared beween Alice and Bob parametrised by the collection of numbers $\boldsymbol{\alpha}$. For our proof, as was discussed before in Chapter 2, the state shared between Alice and Bob ρ_{AB} is purified by adding an ancillary system E possessed by some external agent, named Eve, such that $\rho_{AB} = \mathrm{Tr}_E(|\psi_{ABE}\rangle\langle\psi_{ABE}|)$ where $|\psi_{ABE}\rangle \in \mathbb{C}^d \otimes \mathscr{H}_B \otimes \mathscr{H}_E$.

Bob's observables

Before finding the explicit forms of Bob's observables that maximally violate our steering inequality (5.1), we show that these generalised observables must correspond to projective measurements. Let us concentrate on Bob's first observable and follow the exact same technique as was used in Chapter 4 from Eqs . (4.38) to (4.42) as the relations (5.40) and (4.38) are identical. First, we apply $Z_d^{d-k} \otimes B_{d-k|0}$ to the relation (5.23) and then recalling that Z_d is unitary as well as that $B_{d-k|0} = B_{k|0}^\dagger$ from (2.22), we obtain that

$$\mathbb{1}_{AE} \otimes (B_{k|0}^\dagger B_{k|0})|\psi_{ABE}\rangle = |\psi_{ABE}\rangle. \tag{5.48}$$

Taking a partial trace over the subsystems AE, we arrive at the following condition

$$(B_{k|0}^\dagger B_{k|0})\rho_B = \rho_B, \tag{5.49}$$

where $\rho_B = \mathrm{Tr}_{AE}[|\psi_{ABE}\rangle\langle\psi_{ABE}|]$. Recall that ρ_B is full-rank and thus it is non-singular and invertible. This allows us to immediately conclude that $B_{k|0}^\dagger B_{k|0} = \mathbb{1}_B$ and consequently $B_{k|0}B_{k|0}^\dagger = \mathbb{1}_B$, and thus $B_{k|0}$ is unitary for any $k = 0,\ldots,d-1$. Now using Fact 1, we can conclude that Bob's measurements are projective, that is, the positive semi-definite operators representing the measurement are mutually orthogonal projectors. Further, the fact that B_0 is projective imposes that $B_{k|0}$ are powers of $B_{1|0}$ [see Chapter 2]. As a consequence, from now on we can simply denote $B_{k|0} = B_0^k$, where $B_0 \equiv B_{1|0}$.

Let us now focus on Bob's second observable and show that it corresponds to a projective measurement too. For this purpose, we refer to the second condition (5.32) and then consider the general representation of any state $|\psi_{ABE}\rangle \in \mathbb{C}^d \otimes \mathscr{H}_B \otimes \mathscr{H}_E$ as in Eq. (5.25)

$$|\psi_{ABE}\rangle = \sum_i \lambda_i |i\rangle_A |e_i\rangle_{BE}, \tag{5.50}$$

where $\lambda_i \geq 0$ and $|e_i\rangle_{BE}$ are vectors that are in general not orthogonal. Now recall that,

we showed in the previous subsection we showed that any state satisfying the condition (5.32) must be locally full-rank. Thus, in the state (5.50), $\lambda_i > 0$ for all i. For simplicity, from here on we drop all the subscripts in the notation of the state. Now, by plugging this state in the condition $\langle\psi_{ABE}|S(\boldsymbol{\alpha})|\psi_{ABE}\rangle = 1$, we obtain [cf. Eq. (5.30)]

$$\sum_{k=0}^{d-1}\sum_{i=0}^{d-1}\lambda_i\lambda_{i-k}\mathrm{Re}\left(\langle e_i|[B_{k|1}\otimes\mathbb{1}_E]|e_{i-k}\rangle\right) = \sum_{i,j=0}^{d-1}\frac{\alpha_i}{\alpha_j}\lambda_j^2. \tag{5.51}$$

Dropping the identity acting on Eve, $\mathbb{1}_E$, for the time being and then using the inequality (5.13) with in $u_i = \lambda_i$ and $v_i = \alpha_i$, we arrive at

$$\sum_{k=0}^{d-1}\sum_{i=0}^{d-1}\lambda_i\lambda_{i-k}\mathrm{Re}\left(\langle e_i|B_{k|1}|e_{i-k}\rangle\right) \geq \left(\sum_{i=0}^{d-1}\lambda_i\right)^2. \tag{5.52}$$

Notice that the term on the right hand side of the above inequality can be expanded as $\left(\sum_{i=0}^{d-1}\lambda_i\right)^2 = \sum_{k=0}^{d-1}\sum_{i=0}^{d-1}\lambda_i\lambda_{i-k}$. As a consequence, we immediately obtain that

$$\sum_{k=0}^{d-1}\sum_{i=0}^{d-1}\lambda_i\lambda_{i-k}\mathrm{Re}\left[\left(\langle e_i|B_{k|1}|e_{i-k}\rangle\right) - 1\right] \geq 0. \tag{5.53}$$

Again, recalling that $B_{k|1}^\dagger B_{k|1} \leq \mathbb{1}_B$ for any k allows us to conclude that $\mathrm{Re}\left(\langle e_i|[B_{k|1}|e_{i-k}\rangle\right) \leq 1$ for any i and k. However, λ_i being non-negative in the inequality (5.52), forces the term inside the square brackets to be 0 for all i,k. Thus, we finally obtain

$$\mathrm{Re}\left(\langle e_i|B_{k|1}|e_{i-k}\rangle\right) = 1. \tag{5.54}$$

As the states $|e_i\rangle$ are normalised, the above condition is satisfied iff $B_{k|1}\otimes\mathbb{1}_E|e_{i-k}\rangle = |e_i\rangle$. For this purpose, we again employ the Cauchy-Schwarz inequality (5.39) where $|u\rangle = |e_i\rangle$ and $|v\rangle = B_{k|1}|e_{i-k}\rangle$ and then the fact that $B_{k|1}^\dagger B_{k|1} \leq \mathbb{1}$ from which we obtain $B_{k|1}\otimes\mathbb{1}_E|e_{i-k}\rangle = e^{i\phi}|e_i\rangle$ for some arbitrary phase ϕ. Again using Eq. (5.54), we get that $\phi = 0$. Now, we multiply this equation with its conjugate transpose, to observe that

$$\langle e_{i-k}|[B_{k|1}^\dagger B_{k|1}\otimes\mathbb{1}_E]|e_{i-k}\rangle = 1. \tag{5.55}$$

for any i,k. This implies that for any k the above condition is satisfied for any i. As a consequence, we arrive at a simple relation for any k

$$\langle e_i|[B_{k|1}^\dagger B_{k|1}\otimes\mathbb{1}_E]|e_i\rangle = 1 \qquad (i = 0,\ldots,d-1). \tag{5.56}$$

Tracing out Eve's subsystem, further implies that $\mathrm{Tr}[B_{k|1}^\dagger B_{k|1}\rho_B^i] = 1$ for all i, where $\rho_B^i =$

$\mathrm{Tr}_E[|e_i\rangle\langle e_i|_{BE}]$. As ρ_B^i is positive and again recalling that $B_{k|1}^\dagger B_{k|1} \leq \mathbb{1}_B$ for any k allows us to conclude that this condition holds true iff $B_{k|1}^\dagger B_{k|1}$ is an identity acting onto the support of ρ_B^i. However, notice that the support of Bob's reduced state $\rho_B = \mathrm{Tr}_{AE}[|\psi\rangle\langle\psi|_{ABE}]$ is in-fact composed of the supports of ρ_B^i's. To see this, we use the decomposition of the state $|\psi\rangle_{ABE}$ given in (5.50) to obtain that

$$\begin{aligned}\rho_B &= \mathrm{Tr}_{AE}\left[\sum_{i,j=0}^{d-1}\lambda_i\lambda_j|i\rangle\langle j|\otimes|e_i\rangle\langle e_j|\right] \\ &= \mathrm{Tr}_E\left[\sum_{i=0}^{d-1}\lambda_i^2|e_i\rangle\langle e_i|\right] = \sum_{i=0}^{d-1}\lambda_i^2\rho_B^i. \end{aligned} \tag{5.57}$$

As a consequence, $B_{k|1}^\dagger B_{k|1}$ is an identity that acts on the entire support of Bob's reduced state ρ_B, and thus we finally have that $B_{k|1}^\dagger B_{k|1} = \mathbb{1}_B$ and consequently $B_{k|1}B_{k|1}^\dagger = \mathbb{1}_B$ for all k. Again, using Fact 1, we can conclude that the second Bob's observable corresponds to projective measurements and hence from here on, we denote $B_{k|1} = B_1^k$, where $B_1 \equiv B_{1|1}$. This completes the part of the proof to show that the maximal violation of the steering inequality (5.1) can only be achieved when Bob's both measurements are projective.

Now, we move onto finding the explicit form of Bob's both observables. Let us first consider the relation (5.43) and then apply $\mathbb{1}_A \otimes B_1$ to it, which after rearranging some terms gives us

$$\gamma(\boldsymbol{\alpha})\sum_{k=1}^{d-1}\left(X_d^k\otimes B_1^{k+1}\right)|\psi_{ABE}\rangle = \left[\left(\mathbb{1}_A - \sum_{k=1}^{d-1}\delta_k(\boldsymbol{\alpha})Z_d^k\right)\otimes B_1\right]|\psi_{ABE}\rangle. \tag{5.58}$$

To simplify the notation, let us introduce the following operator

$$\overline{Z}_A := \mathbb{1}_A - \sum_{k=1}^{d-1}\delta_k(\boldsymbol{\alpha})Z_d^k. \tag{5.59}$$

Now, an application of $Z_d^{-1}\otimes\mathbb{1}_B$ to the left hand side of Eq. (5.58) gives us

$$\gamma(\boldsymbol{\alpha})\sum_{k=1}^{d-1}\left(Z_d^{-1}X_d^k\otimes B_1^{k+1}\right)|\psi_{ABE}\rangle = (\overline{Z}_A Z_d^{-1}\otimes B_1)|\psi_{ABE}\rangle, \tag{5.60}$$

where we can interchange the positioning of Z_d and $\overline{Z}_A$ as they commute. Then, by using the commutation relation $Z_dX_d = \omega X_dZ_d$, we can rewrite Eq. (5.60) as

$$\gamma(\boldsymbol{\alpha})\sum_{k=1}^{d-1}\left(\omega^{-k}X_d^k\otimes B_1^{k+1}\right)\left(Z_d^{-1}\otimes\mathbb{1}_B\right)|\psi_{ABE}\rangle = \left(\overline{Z}_A\otimes B_1\right)\left(Z_d^{-1}\otimes\mathbb{1}_B\right)|\psi_{ABE}\rangle, \tag{5.61}$$

where we again used the fact that $Z_d^{-1} \otimes \mathbb{1}_B$ and $\mathbb{1}_A \otimes B_1$ commute. Now, using Eq. (5.40) for $k = 1$, that is, $\left(Z_d^{-1} \otimes \mathbb{1}_B\right) |\psi_{ABE}\rangle = \mathbb{1}_A \otimes B_0 |\psi_{ABE}\rangle$, we finally get

$$\gamma(\boldsymbol{\alpha}) \sum_{k=1}^{d-1} \left(\omega^{-k} X_d^k \otimes B_1^{k+1} B_0\right) |\psi_{ABE}\rangle = (\overline{Z}_A \otimes B_1 B_0) |\psi_{ABE}\rangle. \tag{5.62}$$

Applying B_0 from the left hand side of the expression (5.58), we obtain

$$\gamma(\boldsymbol{\alpha}) \sum_{k=1}^{d-1} \left(X_d^k \otimes B_0 B_1^{k+1}\right) |\psi_{ABE}\rangle = (\overline{Z}_A \otimes B_0 B_1) |\psi_{ABE}\rangle. \tag{5.63}$$

In the next step, we multiply ω^{-1} to Eq. (5.62) and then subtract it from Eq. (5.63), which immediately gives us

$$\gamma(\boldsymbol{\alpha}) \sum_{k=1}^{d-1} \left[X_d^k \otimes \left(B_0 B_1^{k+1} - \omega^{-(k+1)} B_1^{k+1} B_0\right)\right] |\psi_{ABE}\rangle = [\overline{Z}_A \otimes (B_0 B_1 - \omega^{-1} B_1 B_0)] |\psi_{ABE}\rangle. \tag{5.64}$$

Let us again consider the relation (5.43) and multiply it by $X_d^{-1} \otimes \mathbb{1}_B$ from the left hand side, which gives us

$$\sum_{k=1}^{d-1} \left(\gamma(\boldsymbol{\alpha}) X_d^{k-1} \otimes B_1^k\right) |\psi_{ABE}\rangle = (X_d^{-1} \overline{Z}_A \otimes \mathbb{1}_B) |\psi_{ABE}\rangle. \tag{5.65}$$

Then, after multiplying $\mathbb{1}_A \otimes B_0$ to the above equation and then taking into account that it commutes with $X_d \otimes \mathbb{1}_B$, it not difficult to see that

$$\sum_{k=1}^{d-1} \left(\gamma(\boldsymbol{\alpha}) X_d^{k-1} \otimes B_0 B_1^k\right) |\psi_{ABE}\rangle = (X_d^{-1} \overline{Z}_A \otimes B_0) |\psi_{ABE}\rangle. \tag{5.66}$$

Now, let us exploit the relation (5.40) for $k = 1$, that is, $\left(Z_d^{-1} \otimes \mathbb{1}_B\right) |\psi_{ABE}\rangle = \mathbb{1}_A \otimes B_0 |\psi_{ABE}\rangle$ and then using the fact that $\overline{Z}_A$ and Z_d commutes, we finally get,

$$\sum_{k=1}^{d-1} \left(\gamma(\boldsymbol{\alpha}) X_d^{k-1} \otimes B_0 B_1^k\right) |\psi_{ABE}\rangle = (X_d^{-1} Z_d^{-1} \overline{Z}_A \otimes \mathbb{1}_B) |\psi_{ABE}\rangle. \tag{5.67}$$

Next, we apply $Z_d^{-1} \otimes \mathbb{1}_B$ to Eq. (5.65) from the left hand side to obtain,

$$\sum_{k=1}^{d-1} \left(\gamma(\boldsymbol{\alpha}) Z_d^{-1} X_d^{k-1} \otimes B_1^k\right) |\psi_{ABE}\rangle = (Z_d^{-1} X_d^{-1} \overline{Z}_A \otimes \mathbb{1}_B) |\psi_{ABE}\rangle. \tag{5.68}$$

Again, by employing the relation $Z_d X_d = \omega X_d Z_d$, the above equation (5.68) can be rewriten

as

$$\sum_{k=1}^{d-1}\left(\gamma(\boldsymbol{\alpha})\omega^{-(k-1)}X_d^{k-1}\otimes B_1^k B_0\right)|\psi_{ABE}\rangle=\left(\omega X_d^{-1}Z_d^{-1}\overline{Z}_A\otimes\mathbb{1}_B\right)|\psi_{ABE}\rangle. \tag{5.69}$$

Notice that in the left hand side of the above equation, we again exploited the relation (5.40) for $k=1$, that is, $\left(Z_d^{-1}\otimes\mathbb{1}_B\right)|\psi_{ABE}\rangle=\mathbb{1}_A\otimes B_0|\psi_{ABE}\rangle$. Now we apply ω^{-1} to the above equation (5.69) and then subtract it from Eq. (5.66) to get

$$\gamma(\boldsymbol{\alpha})\sum_{k=1}^{d-1}\left[X_d^{k-1}\otimes\left(B_0B_1^k-\omega^{-k}B_1^kB_0\right)\right]|\psi_{ABE}\rangle=0, \tag{5.70}$$

which can be divided up into two parts by separating the term corresponding to $k=1$, as follows

$$\gamma(\boldsymbol{\alpha})\sum_{k=2}^{d-1}\left[X_d^{k-1}\otimes\left(B_0B_1^k-\omega^{-k}B_1^kB_0\right)\right]|\psi_{ABE}\rangle=-\gamma(\boldsymbol{\alpha})\left(B_0B_1-\omega^{-1}B_1B_0\right)|\psi_{ABE}\rangle. \tag{5.71}$$

Notice that the left hand side of the expressions (5.64) and (5.71) are identical, which immediately allows us to get that

$$\overline{Z}_A\otimes(B_0B_1-\omega^{-1}B_1B_0)|\psi_{ABE}\rangle=-\gamma(\boldsymbol{\alpha})\left(B_0B_1-\omega^{-1}B_1B_0\right)|\psi_{ABE}\rangle, \tag{5.72}$$

which after a simple rearrangement of the terms and expanding $\overline{Z}_A$ from (5.59) yields,

$$\left[(1+\gamma(\boldsymbol{\alpha}))\mathbb{1}_A-\sum_{k=1}^{d-1}\delta_k(\boldsymbol{\alpha})Z_d^k\right]\otimes\left(B_0B_1-\omega^{-1}B_1B_0\right)|\psi_{ABE}\rangle=0. \tag{5.73}$$

As proven in Observation 5.1 stated in Appendix C, the operator $[1+\gamma(\boldsymbol{\alpha})]\mathbb{1}-\sum_{k=1}^{d-1}\delta_k(\boldsymbol{\alpha})Z_d^k$ is invertible. Thus, taking trace over the subsystems A,E allows us to finally conclude that

$$(B_0B_1-\omega^{-1}B_1B_0)\rho_B=0, \tag{5.74}$$

where $\rho_B=\mathrm{Tr}_{AE}|\psi_{ABE}\rangle\langle\psi_{ABE}|$. Recalling that ρ_B is full-rank and thus invertible, the above expression (5.74) implies the following commutation relation between Bob's both observables

$$B_0B_1=\omega^{-1}B_1B_0. \tag{5.75}$$

As stated in Fact 2 which was proven in Ref. [31], the above relation along with the fact that $B_0^d=B_1^d=\mathbb{1}_B$ imposes that Bob's Hilbert space decomposes into a tensor product $\mathscr{H}_B=(\mathbb{C}^d)_{B'}\otimes\mathscr{H}_{B''}$ where $\mathscr{H}_{B''}$ is some Hilbert space of unknown but finite dimension.

Along with it, there also exists a unitary transformation $U_B : \mathscr{H}_B \to \mathscr{H}_B$ such that

$$U_B B_0 U_B^\dagger = Z_d^* \otimes \mathbb{1}_{B''}, \quad U_B B_1 U_B^\dagger = X_d \otimes \mathbb{1}_{B''}, \tag{5.76}$$

where $\mathbb{1}_{B''}$ is the identity acting on $\mathscr{H}_{B''}$. This completes the characterisation of Bob's observables that maximally violate the steering inequality (5.1).

The state

We finally have all the tools required to find the state that maximally violates the steering inequality (5.1). As was derived in the previous part, up to a local unitary Bob's both observables are the ideal ones (5.76). Thus, we can rewrite the relation (5.23) and (5.32) by plugging in Bob's derived observables as

$$(Z_d \otimes Z_d^\dagger \otimes \mathbb{1}_{B''E})|\tilde{\psi}_{ABE}\rangle = |\tilde{\psi}_{ABE}\rangle, \tag{5.77}$$

and

$$\sum_{k=1}^{d-1} \left[\gamma(\boldsymbol{\alpha}) X_d^k \otimes X_d^k \otimes \mathbb{1}_{B''E} + \delta_k(\boldsymbol{\alpha}) Z_d^k \otimes \mathbb{1}_{BE}\right] |\tilde{\psi}_{ABE}\rangle = |\tilde{\psi}_{ABE}\rangle, \tag{5.78}$$

where $|\tilde{\psi}_{ABE}\rangle = U_B \otimes \mathbb{1}_{AE}|\psi_{ABE}\rangle$. From here on, for convenience we drop the all the identities from the above relations. As concluded in the previous part of the proof that Bob's Hilbert space is of dimension $(\mathbb{C}^d)_{B'} \otimes \mathscr{H}_{B''}$ due to which the state $|\tilde{\psi}_{ABE}\rangle$ belongs to $(\mathbb{C}^d)_A \otimes (\mathbb{C}^d)_{B'} \otimes \mathscr{H}_{B''} \otimes \mathscr{H}_E$. As a consequence, any such state can be written using the computational basis in $\mathbb{C}^d$ as,

$$|\tilde{\psi}_{ABE}\rangle = \sum_{i,j=0}^{d-1} |i\rangle_A |j\rangle_{B'} |\psi_{ij}\rangle_{B''E}, \tag{5.79}$$

where $|\psi_{ij}\rangle_{B''E}$ is some unnormalised state belonging to $\mathscr{H}_{B''} \otimes \mathscr{H}_E$. After plugging this state to the condition (5.77) for $k = 1$, we arrive at

$$\sum_{i,j=0}^{d-1} \omega^{i-j} |ij\rangle |\psi_{ij}\rangle = \sum_{i,j=0}^{d-1} |ij\rangle |\psi_{ij}\rangle, \tag{5.80}$$

which holds true if and only if $|\psi_{ij}\rangle = 0$ for any $i \neq j$. As a consequence, the only terms in the state (5.79) remains when $i = j$, and thus we have the simplified form of the state given by

$$|\tilde{\psi}_{ABE}\rangle = \sum_{i=0}^{d-1} |ii\rangle |\psi_{ii}\rangle. \tag{5.81}$$

Let us now consider the condition (5.78) where we can extend the range of the sum to $k=0$ by recalling that the $0-th$ power of an observable is identity and also that $\delta_0(\boldsymbol{\alpha})=-1$. Thus, after some rearrangement of the terms we get the following expression

$$\sum_{k=0}^{d-1}\left[\gamma(\boldsymbol{\alpha})X_d^k\otimes X_d^k+\delta_k(\boldsymbol{\alpha})Z_d^k\otimes\mathbb{1}_B\right]|\tilde{\psi}_{ABE}\rangle=\gamma(\boldsymbol{\alpha})|\tilde{\psi}_{ABE}\rangle. \tag{5.82}$$

Plugging in the simplified form of $|\tilde{\psi}_{ABE}\rangle$ as derived in (5.81), the above expression turns out to be

$$\gamma(\boldsymbol{\alpha})\sum_{k=0}^{d-1}\sum_{i=0}^{d-1}|i+k\rangle|i+k\rangle|\psi_{ii}\rangle+\sum_{k=0}^{d-1}\sum_{i=0}^{d-1}\omega^{ki}\delta_k(\boldsymbol{\alpha})|ii\rangle|\psi_{ii}\rangle=\gamma(\boldsymbol{\alpha})\sum_{i=0}^{d-1}|ii\rangle|\psi_{ii}\rangle. \tag{5.83}$$

Mulitplying the above expression with $\langle ss|$ from the lest hand side, we obtain that

$$\sum_{k=0}^{d-1}\gamma(\boldsymbol{\alpha})|\psi_{s\ominus k,s\ominus k}\rangle+\sum_{k=0}^{d-1}\omega^{ks}\delta_k(\boldsymbol{\alpha})|\psi_{ss}\rangle=\gamma(\boldsymbol{\alpha})|\psi_{ss}\rangle \tag{5.84}$$

where $s\ominus k$ represents $s-k$ modulo d. We can simplify the above expression by substituting the explicit form of $\delta(\boldsymbol{\alpha})$ to obtain

$$\sum_{k=0}^{d-1}|\psi_{s\ominus k,s\ominus k}\rangle-\sum_{k=0}^{d-1}\frac{\omega^{k(d-j+s)}}{d}\sum_{\substack{i,j=0\\ i\neq j}}^{d-1}\frac{\alpha_i}{\alpha_j}|\psi_{ss}\rangle=|\psi_{ss}\rangle \tag{5.85}$$

Now, using the identity $\sum_{k=0}^{d-1}\omega^{k(j-s)}=d\delta_{j,s}$, we can simplify the above expression to find the explicit form of the state $|\psi_{ss}\rangle$ given by

$$|\psi_{ss}\rangle=\frac{\alpha_s}{\alpha_0+\ldots+\alpha_{d-1}}|\Psi\rangle, \tag{5.86}$$

where we denoted $|\Psi\rangle=\sum_{k=0}^{d-1}|\psi_{s\ominus k,s\ominus k}\rangle\equiv\sum_{k=0}^{d-1}|\psi_{kk}\rangle$ for any s. As a consequence, Eq. (5.81) can be rewritten as

$$(U_B\otimes\mathbb{1}_{AE})|\psi_{ABE}\rangle \;=\; \left(\sum_{m=0}^{d-1}\alpha_i|ii\rangle_{AB'}\right)\otimes|\xi\rangle_{B''E}=|\psi(\boldsymbol{\alpha})\rangle_{AB'}\otimes|\xi\rangle_{B''E}, \tag{5.87}$$

where

$$|\xi\rangle_{B''E}=\frac{1}{\alpha_0+\ldots+\alpha_{d-1}}|\Psi\rangle. \tag{5.88}$$

This finally completes the proof of certification of all pure bipartite entangled states along with a pair of arbitrary outcome mutually unbiased bases in the 1SDI scenario. □

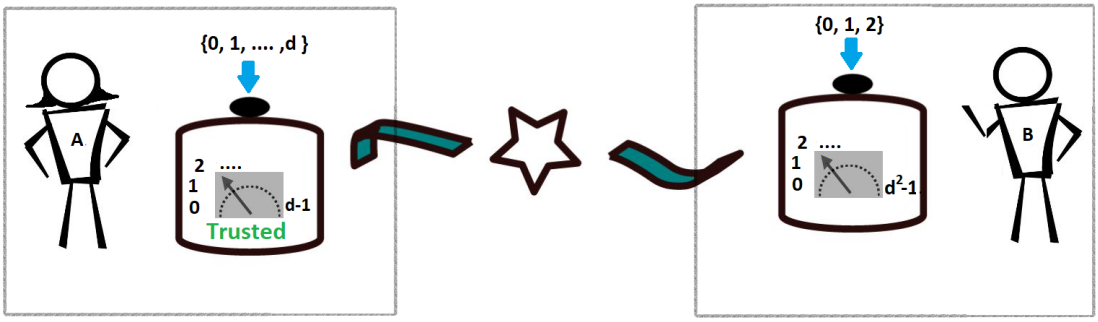


Figure 5.1: 1SDI scenario to certify any rank-one extremal POVM: Alice and Bob receive subsystems from the preparation device on which they perform $d+1$ and 3 measurements respectively such that Alice is trusted. All the measurements are $d-$outcome except Bob's third measurement which is of d^2-outcome.

Let us now proceed towards another important result of this chapter that utilises the above theorem (5.2) involving certification of every rank-one extremal POVM's.

5.4 Certification of all rank-one extremal POVM

As discussed before in Chapter 2, let us consider a rank-one extremal measurement denoted as $\mathscr{I} = \{\mathscr{I}_b\}$, such that b represents its outcomes and $\mathscr{I}_b$ represents the measurement operator corresponding to the $b-th$ outcome. These measurement operators are positive semi-definite and sum up to one. Additionally, it was shown in [70] that measurement operators of an extremal rank-one POVM are projectors scaled down by some non-negative real number, that is, $\mathscr{I}_b = \lambda_b|\mu\rangle\langle\mu|$ with $|\mu\rangle \in \mathbb{C}^d$ and $0 \leq \lambda_b \leq 1$.

It turns our that the observation of the maximal violation of our steering inequality (5.1) plus an additional set of conditions enables us to design a simple method that can be used for certification of any extremal rank-one POVM. For this purpose, we again consider the 1SDI setting such that Alice is again trusted but now performs $d+1$ measurements corresponding to the observables $A_0 = Z_d$ and $A_{i+1} = X_d Z_d^i$ for $i = 0, 1, \ldots, d-1$. Bob is untrusted and performs three measurements, where the first two measurements are $d-$outcome and the third one has d^2-outcomes. The scenario is depicted in Fig. 5.1.

Notice that the statistics corresponding to both Alice and Bob choosing the input $0, 1$, allow us to employ the steering inequality (5.1) and certify any pure bipartite entangled state using Theorem 5.2. Without loss of generality, Bob's third measurement, which is a d^2-outcome POVM, is denoted as $\{R_b\}$. Further, notice that the operators $X_d Z_d^i$ for

$i = 1, 2, \ldots, d-1$ are not proper observables based on the definition introduced in Chapter 2 as $(X_d Z_d^i)^d = \omega^{id(d-1)}\mathbb{1}$. Thus, dividing the matrices with the scalar $\omega^{-i(d-1)}$ yields proper observables, but for simplicity we would drop this factor from further considerations. It is also worth noting that the statistics obtained from the $d+1$ observables, Z_d and $X_d Z_d^i$, are enough to simulate the statistics corresponding to the operators $X_d^i Z_d^j$ for $i, j = 0, 1, \ldots, d-1$ that represent the Heisenberg-Weyl (HW) basis [168] [2]. The reason for this fact is that every element in the HW basis can be generated by considering the powers of Z_d and $X_d Z_d^i$ for all i and then multiply them with appropriate powers of ω. For instance, $X_d^2 Z_d^2$ can be generated by taking $X_d Z_d$ two times and then multiplying it with ω^{-1}, that is, $X_d^2 Z_d^2 = \omega^{-1}(X_d Z_d)^2$. The result is stated below as a simple theorem.

Theorem 5.3. *Assume that Alice and Bob perform the quantum steering experiment and are able to certify that the state shared among them as well as the measurements along with the Hilbert space of Bob as given in Theorem-5.2. Consider then a POVM $R = \{R_b\}$ acting on $\mathscr{H}_B = (\mathbb{C}^d)_{B'} \otimes \mathscr{H}_{B''}$. If for some extremal POVM $\mathscr{I} = \{\mathscr{I}_b\}$ acting on $\mathbb{C}^d$ the following identities*

$$\langle X^i Z^j \otimes R_b \otimes \mathbb{1}_E \rangle_{|\psi_{ABE}\rangle} = \langle X^i Z^j \otimes \mathscr{I}_b \rangle_{|\psi(\boldsymbol{\alpha})\rangle} \tag{5.89}$$

hold true for any $i, j = 0, \ldots, d-1$, where $|\psi_{ABE}\rangle = (\mathbb{1}_A \otimes U_B^\dagger)|\psi(\boldsymbol{\alpha})\rangle_{AB'} \otimes |\xi_{B''E}\rangle$ from (5.46) where $|\psi(\boldsymbol{\alpha})\rangle_{AB'}$ is the ideal state defined in Eq. (5.35). Then, there exist a unitary transformation $U_B : \mathscr{H}_B \to \mathscr{H}_B$ such that the measurement operators of the POVM R are equivalent to the measurement operators of the ideal POVM $\mathscr{I}$ as

$$U_B \; R_b \; U_B^\dagger = \mathscr{I}_b \otimes \mathbb{1}_{B''} \qquad \forall b. \tag{5.90}$$

Proof. Our proof takes inspiration from the technique introduced in Ref. [41], where extremal POVM's acting on two-dimensional Hilbert space were certified up to certain equivalences. Here, we generalise that approach to POVM's that act on arbitrary dimensional Hilbert space in the scenario where Alice is trusted. Let us first observe that the statistics one observes from the actual experiment must be equivalent to one observed in the ideal experiment, that is,

$$\forall\; b \quad \forall i, j \qquad \langle \psi_{ABE} | X^i Z^j \otimes R_b \otimes \mathbb{1}_E | \psi_{ABE} \rangle = \langle \psi(\boldsymbol{\alpha}) | X^i Z^j \otimes \mathscr{I}_b | \psi(\boldsymbol{\alpha}) \rangle. \tag{5.91}$$

Solving the above condition is enough to certify the POVM R. For this purpose, as was done in Chapter 4, we first rewrite the state $|\psi(\boldsymbol{\alpha})\rangle$ in terms of the maximally entangled

[2] The HW basis is a collection of operators that forms a basis for operators that act on $d-$dimensional Hilbert space with d being any positive integer.

state of two qudits $|\phi_+^d\rangle$ [see Eq. (4.16)] as

$$|\psi(\boldsymbol{\alpha})\rangle = [\mathbb{1}_A \otimes P(\boldsymbol{\alpha})]|\phi_+^d\rangle, \tag{5.92}$$

where

$$P(\boldsymbol{\alpha}) = \sum_{i=0}^{d-1} \alpha_i |i\rangle\langle i|. \tag{5.93}$$

Recall that $\alpha_i > 0$ for all i and $\sum_i \alpha_i^2 = 1$. Let us also introduce another set of d^2 number of operators, derived from HW basis

$$W_{i,j} := P(\boldsymbol{\alpha})^{-1} \left(X^i Z^j\right)^* P(\boldsymbol{\alpha})^{-1}. \tag{5.94}$$

Let us observe that the above operators are linearly independent as $P(\boldsymbol{\alpha})$ is invertible and $X^i Z^j$ are orthogonal in the Hilbert-Schmidt scalar product, that is, $\mathrm{Tr}[X^i Z^j (X^{i'} Z^{j'})^\dagger] = d\delta_{i,i'}\delta_{j,j'}$. As a consequence, the set $\{W_{i,j}\}$ forms a complete basis for operators acting on $d-$dimensional Hilbert space. Recalling that the measurement operators $\mathscr{I}_b$ of the ideal POVM act on $d-$dimensional Hilbert space and thus, using the newly defined operator basis (5.94), we can express them as

$$\mathscr{I}_b = \sum_{i,j=0}^{d-1} l_{i,j}^b W_{i,j} \qquad \forall b, \tag{5.95}$$

where $l_{i,j}^b$ are in general complex coefficients. Let us now compute the right hand side of the expression (5.91) by plugging in the above representation of the POVM $\mathscr{I}$,

$$\begin{aligned} \langle\psi(\boldsymbol{\alpha})|X^i Z^j \otimes \mathscr{I}_b|\psi(\boldsymbol{\alpha})\rangle &= \sum_{m,n} l_{m,n}^b \langle\psi(\boldsymbol{\alpha})|X^i Z^j \otimes P(\boldsymbol{\alpha})^{-1} \left(X^m Z^n\right)^* P(\boldsymbol{\alpha})^{-1}|\psi(\boldsymbol{\alpha})\rangle \\ &= \sum_{m,n} l_{m,n}^b \langle\phi_+^d|X^i Z^j \otimes \left(X^m Z^n\right)^*|\phi_+^d\rangle, \end{aligned} \tag{5.96}$$

where we exploited the form of the state $|\psi(\boldsymbol{\alpha})\rangle$ given in (5.92). Now, exploiting the identity $(R \otimes Q)|\phi_+^d\rangle = (RQ^T \otimes \mathbb{1})|\phi_+^d\rangle$ that is satisfied for any two matrices Q and R acting on $d-$dimensional Hilbert space [see Fact 5 in Appendix A] and also the fact that $X^i Z^j$ form an orthogonal basis as mentioned above, we finally obtain that

$$\langle\psi(\boldsymbol{\alpha})|X^i Z^j \otimes \mathscr{I}_b|\psi(\boldsymbol{\alpha})\rangle = l_{i,j}^b \qquad \forall b. \tag{5.97}$$

Next, our aim is to compute the left hand side of the expression (5.91). We use the fact that according to Theorem 5.2, Bob's Hilbert space decomposes as $\mathscr{H}_B = \mathbb{C}^d \otimes \mathscr{H}_{B''}$ and there exist a unitary $U_B : \mathscr{H}_B \to \mathscr{H}_B$ that transforms that transforms the state $|\psi_{ABE}\rangle$

as

$$(\mathbb{1}_{AE} \otimes U_B)|\psi_{ABE}\rangle = |\psi(\boldsymbol{\alpha})\rangle_{AB'} \otimes |\xi_{B''E}\rangle. \tag{5.98}$$

Now, any measurement operator of the POVM R acting on $\mathscr{H}_B$ can be expressed using the basis (5.94) as,

$$U_B R_b U_B^\dagger = \sum_{i,j=0}^{d-1} W_{i,j} \otimes \widetilde{R}_{i,j}^b, \tag{5.99}$$

where $\widetilde{R}_{i,j}^b$ are general operators acting on $\mathscr{H}_{B''}$. Now, computing the left hand side of (5.91) by plugging in it the above mentioned form of R_b (5.99) and the state $|\psi_{ABE}\rangle$, we have

$$\langle\psi_{ABE}|X^i Z^j \otimes R_b \otimes \mathbb{1}_E|\psi_{ABE}\rangle = \left[\sum_{m,n}\langle\psi(\boldsymbol{\alpha})|X^i Z^j \otimes W_{m,n}|\psi(\boldsymbol{\alpha})\rangle\right]\langle\xi_{B''E}|\widetilde{R}_{i,j}^b \otimes \mathbb{1}_E|\xi_{B''E}\rangle. \tag{5.100}$$

As was computed above to get (5.97) from (5.96), the term inside the square bracket in the above expression is just 1. Thus, we finally arrive at

$$\langle\psi_{ABE}|X^i Z^j \otimes R_b \otimes \mathbb{1}_E|\psi_{ABE}\rangle = \langle\xi_{B''E}|\widetilde{R}_{i,j}^b \otimes \mathbb{1}_E|\xi_{B''E}\rangle = \mathrm{Tr}\left(\widetilde{R}_{i,j}^b \sigma_{B''}\right) \qquad \forall b, \tag{5.101}$$

where $\sigma_{B''} = \mathrm{Tr}_E(|\xi_{B''E}\rangle\langle\xi_{B''E}|)$. Let us now decompose $\sigma_{B''}$ using its eigenvectors denoted by $|k\rangle$ as $\sigma_{B''} = \sum_k p_k|k\rangle\langle k|$. Plugging this into the above expression, we get that

$$\mathrm{Tr}\left(\widetilde{R}_{i,j}^b \sigma_{B''}\right) = \sum_k p_k \langle k|\widetilde{R}_{i,j}^b|k\rangle. \tag{5.102}$$

Recalling again the identity (5.91) and then using Eq. (5.97), we finally arrive at

$$\sum_k p_k \langle k|\widetilde{R}_{i,j}^b|k\rangle = l_{i,j}^b. \tag{5.103}$$

Next, we introduce a family of POVM's k as, $\mathscr{I}_k = \{\mathscr{I}_{b,k}\}$, whose measurement operators are given by

$$\begin{aligned} \mathscr{I}_{b,k} &= \mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes |k\rangle\langle k|_{B''})\, R_b\right] \\ &= \sum_{i,j=0}^{d-1} \langle k|\widetilde{R}_{i,j}^b|k\rangle W_{i,j}. \end{aligned} \tag{5.104}$$

As R is a valid POVM, as discussed in Chapter 2 all its measurement operators are hermitian and positive semi-definite, that is, $R_b \geq 0$ for all b. Consequently, from the first

line of Eq. (5.104), we can see that $\mathscr{I}_{b,k}$ is also positive semi-definite, that is, $\mathscr{I}_{b,k} \geq 0$ for any k and b, as product of two positive semi-definite matrices is also positive semi-definite. Further, $\sum_b R_b = \mathbb{1}_B$ is identity and then using the first line of of Eq. (5.104), we can directly see that $\sum_b \mathscr{I}_{b,k} = \mathbb{1}_{B'}$ for any k. As a consequence, the family of POVM's $\{\mathscr{I}_b^k\}_b$ are valid quantum measurements. Let us now go back to Eq. (5.103), and then rewrite it using the family of POVM's (5.104) as

$$\mathscr{I}_b = \sum_{i,j=0}^{d-1} l_{i,j}^b W_{i,j} = \sum_{i,j=0}^{d-1} \sum_k p_k \langle k|\widetilde{R}_{i,j}^b|k\rangle W_{i,j} = \sum_k p_k \mathscr{I}_{b,k}. \tag{5.105}$$

However, the POVM $\mathscr{I}$ is extremal and can not be decomposed as a convex mixture of other POVM's. Thus, we can immediately conclude that

$$\forall k \qquad \mathscr{I}_{b,k} = \mathscr{I}_b, \tag{5.106}$$

which is equivalent to the condition,

$$\forall k \qquad \langle k|\widetilde{R}_{i,j}^b|k\rangle = l_{i,j}^b. \tag{5.107}$$

Next, we consider the following vectors belonging to $\mathbb{C}^d$:

$$|\varphi_{a,s,t}\rangle = \frac{1}{\sqrt{2}}\left(|s\rangle \pm \mathbb{i}^a |t\rangle\right), \tag{5.108}$$

where $a = 0, 1$ and $|s\rangle$ and $|t\rangle$ are two distinct vectors belonging to the eigenbasis $\{|k\rangle\}$ of $\sigma_{B''}$. We now compute the following quantity

$$\mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes |\varphi_{a,s,t}\rangle\langle\varphi_{a,s,t}|_{B''})\, R_b\right] = \sum_{i,j} \mathrm{Tr}(|\varphi_{a,s,t}\rangle\langle\varphi_{a,s,t}|_{B''} \widetilde{R}_{i,j}^b) W_{i,j}. \tag{5.109}$$

Expanding the above quantity using the explicit form of the vectors given in (5.108), we obtain

$$\mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes |\varphi_{a,s,t}\rangle\langle\varphi_{a,s,t}|_{B''})\, R_b\right] = \mathscr{I}_b \pm \mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L_{B''}^a) R_b\right], \tag{5.110}$$

where

$$L_{B''}^a = (\mathbb{i}^a/2)\left(|t\rangle\langle s| + (-1)^a |s\rangle\langle t|\right). \tag{5.111}$$

The fact that $R_b \geq 0$, imposes that left-hand side of the above expression is non-negative as it is a product of two matrices that are positive semi-definite matrices. This allows us

to conclude that

$$\mathscr{I}_b \geq \pm \mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right]. \tag{5.112}$$

As discussed above, the measurement operators of any rank-one extremal POVM acting on $d-$dimensional Hilbert space can be expressed as $\mathscr{I}_b = \lambda_b |\mu_b\rangle\langle\mu_b|$, where the vectors $|\mu_b\rangle$ are normalized and belong to $\mathbb{C}^d$. Using this fact, we show in Observation 5.2 stated in Appendix C that the operator appearing on the right-hand side of the above expression (5.112) must be rank one as well and must admit the following form

$$\mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right] = \lambda'_b |\mu_b\rangle\langle\mu_b|, \tag{5.113}$$

such that $\lambda_b \geq \pm\lambda'_b$. Recalling that $\sum_b R_b = \mathbb{1}_B$ and that $\mathrm{Tr}L^a_{B''} = 0$ for any a, we can finally conclude that

$$\sum_b \mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right] = 0 = \sum_b \lambda'_b |\mu_b\rangle\langle\mu_b|. \tag{5.114}$$

Since $\mathscr{I}_b$ are linearly independent, we learn from the above condition that $\lambda'_b = 0$ for all b which in turn implies from (5.113) that $\mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right] = 0$ for any b and a. Finally expanding the left hand side of (5.113) by plugging in the explicit form of $L^a_{B''}$ and also taking into account that $X^i Z^j$ are linearly independent for any i, j gives us two simple conditions:

$$\left(X^i Z^j\right)^* \left(\langle s|\widetilde{R}^b_{i,j}|t\rangle + \langle t|\widetilde{R}^b_{i,j}|s\rangle\right) = 0, \tag{5.115}$$

for $a = 0$ and

$$\left(X^i Z^j\right)^* \left(\langle t|\widetilde{R}^b_{i,j}|s\rangle - \langle s|\widetilde{R}^b_{i,j}|t\rangle\right) = 0, \tag{5.116}$$

for $a = 1$. One can immediately see that the only possible solution of the above conditions (5.115) and (5.116) is $\langle s|\widetilde{R}^b_{i,j}|t\rangle = 0$ for $s \neq t$. Thus, from Eq. (5.107) we can conclude that the POVM acting on the support of Bob's local state is given by $R_b = \mathscr{I}_b \otimes \mathbb{1}_{B''}$ for all $b's$. This completes the proof. □

It is worth noting that the above certification scheme works for any rank-one extremal POVM with arbitrary number of outcomes. However, it was shown in [70] that any extremal POVM with d^2 outcomes have to be rank-one. As a consequence, we certify every d^2-outcome extremal POVM. We now show that the certified state and the certified POVM can be used for optimal randomness certification.

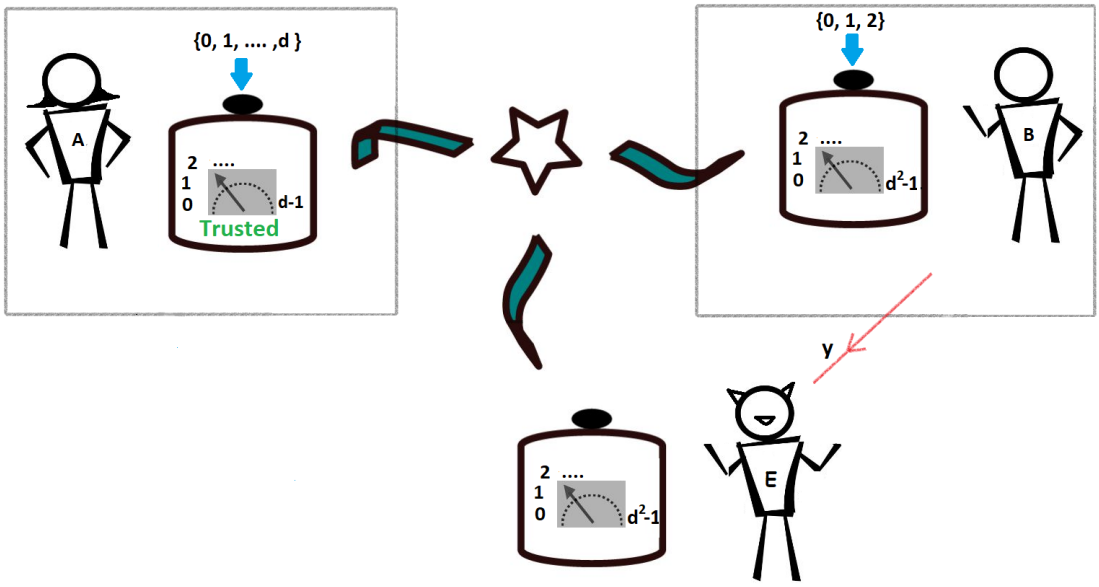


Figure 5.2: Optimal randomness certification in the 1SDI scenario: Alice (trusted) and Bob receive subsystems from the preparation device on which they perform $d+1$ and 3 measurements respectively. All the measurements are $d-$outcome except Bob's third measurement which has d^2 outcomes. Using this measurement Bob wishes to generate $2\log_2 d$ bits of randomness. Eve has knowledge about Bob's measurement choices. She also might receive an additional system from the preparation device. Using her measuring device and the received subsystem from the preparation she wants to guess Bob's outcome.

5.5 Optimal randomness certification

Let us again go back to the previous scenario depicted in Fig. 5.1, but now let us assume that there is another party Eve who wants to guess Bob's outcome. As discussed in Chapter 2, Eve has full control on Bob's lab and also has access to the state sent by the preparation device. However, unlike randomness certification in the Bell scenario, in the 1SDI scenario Eve has no access to Alice's lab as it is trusted. This is depicted in Fig. 5.2.

Let us now say that Alice and Bob observe the maximal violation of the steering inequality (5.1) using the observables corresponding to the inputs $x, y = 0, 1$ where $A_0 = Z_d$ and $A_1 = X_d$. Now, using Theorem 5.2, Alice and Bob can certify the quantum state shared between Alice and Bob up to local unitaries and additional degrees of freedom [see Eq. (5.46)]. Notice that in the proof we considered an external system E that was used to purify the state shared between Alice and Bob. Without loss of generality, this external system in fact denotes the subsystem possessed by Eve and her Hilbert space is denoted by

$\mathscr{H}_E$. Again, in the previous section, using this result we certified Bob's third measurement to be an ideal extremal measurement up to some local unitary [see Eq. (5.90)]. Notice that in the proof, the only condition we used apart from Theorem 5.2 was that the statistics one obtains in the actual experiment is the same as in the ideal experiment, even with the presence of the external subsystem E which is held with Eve [cf. Eq. (5.91)]. Given the certified state and the measurements, let us now compute the probability of Eve to guess Bob's outcomes corresponding to the POVM R [cf. Chapter 2],

$$\begin{aligned} G(y=2,\vec{p}) &= \sup_{S_p} \sum_b \langle \psi_{ABE} | \mathbb{1}_A \otimes R_b \otimes E^{(b)} | \psi_{ABE} \rangle \\ &= \sup_{S_p} \langle \psi(\boldsymbol{\alpha}) | \mathbb{1}_A \otimes \mathscr{I}_b | \psi(\boldsymbol{\alpha}) \rangle \langle \xi_{B''E} | \mathbb{1}_{B''} \otimes E^{(b)} | \xi_{B''E} \rangle. \end{aligned} \tag{5.117}$$

Eve's strategy is composed of the states $\sigma_E = \mathrm{Tr}_{B''} |\xi_{B''E}\rangle\langle\xi_{B''E}|$ and a measurement $Z = \{E^{(b)}\}$. Thus, simplifying the above expression we obtain

$$G(y=2,\vec{p}) = \sup_{\sigma_E, Z} \sum_b \mathrm{Tr}[\mathscr{I}_b \rho_{B'}(\boldsymbol{\alpha})] \mathrm{Tr}[E^{(b)} \sigma_E] \tag{5.118}$$

where $\rho_{B'}(\boldsymbol{\alpha}) = \mathrm{Tr}_A |\psi(\boldsymbol{\alpha})\rangle\langle\psi(\boldsymbol{\alpha})|_{AB'}$. Using the fact $\sum_b E^{(b)} = \mathbb{1}_E$, we can immediately observe from the above expression that for any extremal POVM $\{\mathscr{I}_b\}$ if

$$\mathrm{Tr}[\mathscr{I}_b \rho_B(\boldsymbol{\alpha})] = \frac{1}{d^2} \qquad \forall b, \tag{5.119}$$

then the guessing probability (5.117) is $G(y=2,\vec{p}) = 1/d^2$. As a consequence, the maximal violation of the steering inequality (5.1) along with with conditions (5.91), can be used to certify $2\log_2 d$ bits of randomness from Bob's POVM using any pure bipartite entangled state provided there exists an extremal POVM $\{\mathscr{I}_b\}$ that satisfies the condition (5.119) for any $\rho_B(\boldsymbol{\alpha})$.

Here we show an example of extremal qudit POVM that can be used to generate the optimal amount of randomness by Bob when he and Alice and share the two-qudit maximally entangled state $|\phi_+^d\rangle$. We consider a simple construction of family of extremal d^2-outcome POVM's acting on arbitrary dimensional Hilbert space introduced in Ref. [70]. It turns out that such POVM's serve as a perfect example to obtain the desired result. Consider the following d^2 unitary operators defined as

$$U_{k,l} = X_d^k Z_d^l, \tag{5.120}$$

where $k,l = 0 \ldots d-1$ and a vector $|v\rangle \in \mathbb{C}^d$ such that $\mathrm{Tr}[U_{k,l}^\dagger |v\rangle] \neq 0$ for any k,l. As

proven in [70], the following d^2-outcome POVM given by

$$\mathscr{I}_{k,l} := \frac{1}{d} U_{k,l}|v\rangle\langle v|U_{k,l}^{\dagger}, \tag{5.121}$$

is extremal. Notice that when $|\psi_{AB}\rangle = |\phi_{+}^{d}\rangle$, then the local states of Alice and Bob are $\rho_A = \rho_B = \mathbb{1}_d/d$. Now, plugging this reduced state and the above POVM (5.121) into the left hand side of the condition (5.119), we see that

$$\mathrm{Tr}[\mathscr{I}_b \rho_B(\boldsymbol{\alpha})] = \frac{1}{d^2}\mathrm{Tr}(U_{k,l}|v\rangle\langle v|U_{k,l}^{\dagger}) = \frac{1}{d^2} \qquad \forall k,l. \tag{5.122}$$

Thus, the example provided above can be used to obtain optimal randomness.

Now, we also demonstrate that the optimal randomness can be certified when Alice and Bob share partially entangled states. For this purpose, we find examples of extremal qudit POVMs with d^2 outcomes when $d = 3,4,5,6$ that can be used to securely generate $2\log_2 d$ amount of random bits using a particular class of partially entangled pure states $|\psi(\boldsymbol{\alpha})\rangle_{AB}$ such that $\alpha_i \geq 1/d$ for $i = 0,1,\ldots,d-2$. These extremal POVM's are given by,

$$\mathscr{I}_b := \lambda_b |\delta_b\rangle\langle\delta_b|. \tag{5.123}$$

For $b = 0,\ldots,d-2$, the vectors $|\delta_b\rangle$ are given by

$$|\delta_b\rangle = |b\rangle, \tag{5.124}$$

whereas, for $b = d-1,\ldots,d^2-1$ they are defined as

$$|\delta_b\rangle = \sum_{i=0}^{d-1} \mu_i \exp\left(\frac{2\pi \mathbb{i}\xi_i(b-d+1)}{d^2-d+1}\right)|i\rangle \tag{5.125}$$

where

$$\mu_i = \sqrt{\frac{1-\lambda_i}{(d^2-d+1)\lambda_d}} \qquad (i = 0,1,\ldots,d-2) \tag{5.126}$$

and

$$\mu_{d-1} = \sqrt{\frac{1}{(d^2-d+1)\lambda_d}}. \tag{5.127}$$

The $\lambda_b's$ are given by

$$\lambda_i = \frac{1}{d^2\alpha_i^2} \qquad (i = 0,1,\ldots,d-2) \tag{5.128}$$

and

$$\lambda_{d-1} = \lambda_d = \ldots = \lambda_{d^2-1} = \frac{1}{d^2-d+1}\left(d - \sum_{i=0}^{d-2} \lambda_i\right). \tag{5.129}$$

Finally, below we provide the ξ_i coefficients.
For $d = 3$:

$$\xi_0 = 0, \quad \xi_1 = 1 \quad \text{and} \quad \xi_2 = 3. \tag{5.130}$$

For $d = 4$:

$$\xi_0 = 0, \quad \xi_1 = 1, \quad \xi_2 = 3 \quad \text{and} \quad \xi_3 = 9. \tag{5.131}$$

For $d = 5$:

$$\xi_0 = 0, \quad \xi_1 = 1, \quad \xi_2 = 4, \quad \xi_3 = 14 \quad \text{and} \quad \xi_4 = 16. \tag{5.132}$$

For $d = 6$:

$$\xi_0 = 0, \quad \xi_1 = 1, \quad \xi_2 = 3, \quad \xi_3 = 8, \quad \xi_4 = 12 \quad \text{and} \quad \xi_4 = 18. \tag{5.133}$$

All these coefficients were found numerically such that the above constructed POVM is extremal and satisfies the condition (5.119).

5.6 Conclusions and Discussions

In this chapter, we first constructed a family of steering inequalities that are maximally violated by every pure entangled bipartite state. The only other work that provides a steering inequality that is maximally violated by any pure entangled state is Ref. [166]. However, the inequality proposed in Ref. [166] requires the trusted party to perform the full tomography on her subsystem. On the other hand, our scheme is the most efficient in terms of the number of measurements, as we require only two measurements to be performed by both the parties. This is the minimal number required to observe any form of quantum non-locality. We then showed that the maximal violation of our inequality allows one to certify any pure bipartite entangled state in the 1SDI scenario. A method for certification of any pure entangled bipartite state in the 1SDI scenario was also proposed in [129], but their approach is a direct translation of the method of Ref. [169] to the 1SDI scenario that relies on certification of two-qubit states as discussed before in Chapter 3. The scheme also requires both the parties to perform three and four measurements respectively. Contrary to this, our certification scheme relies only on two

genuinely d-outcome measurements per party making it extremely useful for experimental implementation. Moreover, our scheme does not need to assume that the state shared among Alice and Bob is pure and the measurements performed by them are projective.

Improving on the results presented in the previous Chapter 4, we went on further with our self-testing result and used it to certify any rank-one extremal POVM in 1SDI scenario. Apart from it, we also showed that this task can be accomplished with quantum states that are close to separable states, that is, quantum states with a low level of entanglement. This makes our scheme resource friendly. Finally, we utilised both these results to devise a simple scheme for certification of the optimal amount of $2\log_2 d$ bits of randomness using quantum systems of local dimension d in the 1SDI scenario. Apart from its importance towards application in quantum cryptography, our result answers a long-standing question in the quantum foundations community of whether one can securely generate this optimal amount of randomness. Moreover, for a few finite dimensions, we showed that we can also accomplish this task using low levels of entanglement.

Some interesting follow-up questions arise from our work. First, and the most important one would be to explore whether our construction of the steering functionals can be used to design Bell functionals whose maximal quantum value is achieved by any pure entangled bipartite state and two measurements per site which can be later used for self-testing. Another interesting problem would be to devise a scheme for certification of extremal measurements of arbitary rank, and thus certify any quantum measurement in the 1SDI scenario. A direct follow-up problem from our work is to find extremal POVM's satisfying the condition (5.119) for any $\rho_B(\boldsymbol{\alpha})$. A more challenging problem would be then to find a fully device-independent scheme for certification of optimal randomness using quantum systems of arbitrary local dimension. For the particular case of $d = 2$ and $d = 3$, schemes have been devised that can certify $2\log_2 2$ and $2\log_2 3$ bits of local randomness in [41] and [42] respectively (see also Ref. [170]).

Chapter 6

Concluding remarks

6.1 Summary of the thesis

Let us finally summarise the major points presented throughout this thesis and their relevance to the current literature in quantum information and foundations.

From a theoretical perspective

1. All the results presented in this thesis are very general, in the sense that, they are applicable to composite quantum systems of arbitrary local dimensions. The results presented in Chapter 3 are even applicable to arbitrary number of parties. As a matter of fact, the results presented in Chapter 4 and Chapter 5 can also be generalised to arbitrary number of parties using similar mathematical techniques.

2. Most of the known certification schemes in the device-independent regime deal with states that are locally qubits and thus can utilise the Jordan's lemma [63] which simplifies the mathematical considerations significantly. Our work is thus interesting from a mathematical point of view, as we develop new mathematical techniques that are applicable to arbitrary finite dimensional quantum systems.

3. The result presented in Chapter 3 provide an interesting insight into the structure of quantum sets. For instance, it was exploited in Ref. [154] to show that the set of quantum correlations in a certain Bell scenario is not closed.

4. An open question in quantum information has been whether one can securely generate the optimal randomness using quantum systems of arbitrary local dimension. In Chapter 5, we show that it is possible in the 1SDI scenario.

From a practical perspective

1. We showed in Chapter 3 that one can certify the generalised GHZ state using just two genuinely $d-$outcome measurements per party in a fully device-independent way. This is the minimum number of measurements required to observe quantum non-locality and thus more efficient as compared to the existing schemes with regards to implementing it in experiments as one needs to observe minimum number of correlations to certify the state.

2. Mutually unbiased bases are essential for quantum cryptographic tasks. In Chapter 4, we presented robust certification of mutually unbiased bases in the 1SDI scenario. This is the first instance where a method for certification of a general family of measurements, termed genuinely incompatible, have been introduced, which is based on quantum steering.

3. In Chapter 5, we demonstrated a method to certify any pure bipartite entangled state using just two genuinely $d-$outcome measurements per party in the 1SDI scenario. This is again the most efficient protocol till date that can be used to certify such states. We then showed that any rank-one extremal measurement can be certified in the 1SDI scenario.

4. Any cryptographic task requires access to sources generating random bits. In Chapter 3, we demonstrated a protocol to generate randomness of amount $\log_2 d$ bits using projective measurements in a fully device-independent way. Then, in Chapter 5, we showed that optimal randomness of amount $2\log_2 d$ bits can be certified using a quantum system and a generalised measurement in the 1SDI scenario. Both of these protocols are secure against any eavesdropper who has access to quantum resources.

Let us list some of the interesting open questions that stem from this work.

6.2 Open questions for further exploration

1. The first open question that naturally stems from this work is to find Bell inequalities inspired from the construction of our steering inequalities in Chapter 5 that are maximally violated by any pure bipartite entangled state and utilises only two measurements per party. Then, building on our techniques described in Chapter 3, it would be extremely interesting to prove self-testing statements of such states in the fully DI scenario using minimal number of measurements.

2. Generalising the steering inequalities in Chapter 5 to the multipartite scenario in order for 1SDI certification of any pure multipartite entangled state. The author of this thesis is currently investigating the possibility to certify certain class of multipartite states in the 1SDI scenario such as graph states and Schmidt states by extending the approach presented in Chapter 4 and Chapter 5.

3. Generalising the certification method of rank-one extremal measurements in the 1SDI scenario to measurements of arbitrary rank. Further, it would be interesting to explore whether one can reduce the number of measurements performed by each party, as in our scheme, the trusted party needs to perform $d+1$ measurements.

4. Finding ideal POVM's that can be used to locally generate the optimal amount of randomness using any pure partially entangled bipartite state, or putting it simply, finding extremal POVM's $\{\mathscr{I}_b\}$ that satisfies the condition (5.91) for any non-singular local state ρ_B.

5. Extending all the 1SDI schemes presented in this thesis to the fully device-independent scenario. In particular, it would be extremely interesting to provide a way to certify the optimal amount of randomness in the fully device-independent scenario. Further, certifying the mutually unbiased bases in a fully device-independent way has been a long sought after question in quantum information community. For instance, if one can fully characterise the trusted side in the scheme presented in Chapter 4, then this scheme becomes fully device-independent.

Bibliography

[1] J. Preskill, "Course information for physics 219/computer science 219 quantum computation," 2015. [Online]. Available: http://theory.caltech.edu/~preskill/ph229/.

[2] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information: 10th anniversary edition," 2010. [Online]. Available: https://doi.org/10.1017/CBO9780511976667.

[3] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" **Phys. Rev.**, vol. 47, 777–780, 10 May 1935. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRev.47.777.

[4] J. S. Bell, "On the einstein-podolsky-rosen paradox," **Physics Physique Fizika**, vol. 1, no. 3, 195, 1964. [Online]. Available: https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195.

[5] A. Aspect, P. Grangier, and G. Roger, "Experimental realization of einstein-podolsky-rosen-bohm gedanken experiment: A new violation of Bell's inequalities," **Phys. Rev. Lett.**, vol. 49, 91–94, 2 Jul. 1982. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.49.91.

[6] A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via Bell's theorem," **Phys. Rev. Lett.**, vol. 47, 460–463, 7 Aug. 1981. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.47.460.

[7] M. Giustina, A. Mech, S.Ramelow, and et al., **Nature**, vol. 497, 227–230, 2013. [Online]. Available: https://doi.org/10.1038/nature12012.

[8] B. Hensen, H. Bernien, A. Dréau, and et al., "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," **Nature**, vol. 526, 682–686, 2015. [Online]. Available: https://doi.org/10.1038/nature15759.

[9] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," **Phys. Rev. Lett.**, vol. 98, 230501, 23 Jun. 2007. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.98.230501.

[10] D. Mayers and A. C.-C. Yao, "Quantum cryptography with imperfect apparatus," **Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)**, 503–509, 1998. [Online]. Available: https://arxiv.org/abs/quant-ph/9809039.

[11] D. Mayers and A. Yao, "Self testing quantum apparatus," **Quantum Inf. Comput.**, vol. 4, no. 4, 273–286, 2004. [Online]. Available: http://dl.acm.org/citation.cfm?id=2011827.2011830.

[12] M McKague, T. H. Yang, and V Scarani, "Robust self-testing of the singlet," **Journal of Physics A: Mathematical and Theoretical**, vol. 45, no. 45, 455304, Oct. 2012. [Online]. Available: https://doi.org/10.1088/1751-8113/45/45/455304.

[13] T. H. Yang and M. Navascués, "Robust self-testing of unknown quantum systems into any entangled two-qubit states," **Phys. Rev. A**, vol. 87, 050102, 5 May 2013. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.87.050102.

[14] C. Bamps and S. Pironio, "Sum-of-squares decompositions for a family of clauser-horne-shimony-holt-like inequalities and their application to self-testing," **Phys. Rev. A**, vol. 91, 052111, 5 May 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.91.052111.

[15] Y. Wang, X. Wu, and V. Scarani, "All the self-testings of the singlet for two binary measurements," **New Journal of Physics**, vol. 18, no. 2, 025021, Feb. 2016. [Online]. Available: https://doi.org/10.1088/1367-2630/18/2/025021.

[16] I Šupić, R Augusiak, A Salavrakos, and A Acín, "Self-testing protocols based on the chained bell inequalities," **New Journal of Physics**, vol. 18, no. 3, 035013, Apr. 2016. [Online]. Available: https://doi.org/10.1088/1367-2630/18/3/035013.

[17] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, "Robust and versatile black-box certification of quantum devices," **Phys. Rev. Lett.**, vol. 113, 040401, 4 Jul. 2014. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.113.040401.

[18] T. Coopmans, J. Kaniewski, and C. Schaffner, "Robust self-testing of two-qubit states," **Phys. Rev. A**, vol. 99, 052123, 5 May 2019. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.99.052123.

[19] J. Kaniewski, "Self-testing of binary observables based on commutation," **Phys. Rev. A**, vol. 95, 062323, 6 Jun. 2017. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.95.062323.

[20] X. Li, Y. Wang, Y. Han, S. Qin, F. Gao, and Q. Wen, "Analytic robustness bound for self-testing of the singlet with two binary measurements," **J. Opt. Soc. Am. B**, vol. 36, no. 2, 457–463, Feb. 2019. [Online]. Available: http://opg.optica.org/josab/abstract.cfm?URI=josab-36-2-457.

[21] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, "Device-independent state estimation based on bell's inequalities," **Phys. Rev. A**, vol. 80, 062327, 6 Dec. 2009. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.80.062327.

[22] M. McKague, "Self-testing graph states," **Theory of Quantum Computation, Communication, and Cryptography**, D. Bacon, M. Martin-Delgado, and M. Roetteler, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, 104–120.

[23] J. Kaniewski, "Analytic and nearly optimal self-testing bounds for the clauser-horne-shimony-holt and mermin inequalities," **Phys. Rev. Lett.**, vol. 117, 070402, 7 Aug. 2016. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.117.070402.

[24] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín, "Scalable bell inequalities for qubit graph states and robust self-testing," **Phys. Rev. Lett.**, vol. 124, 020402, 2 Jan. 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.124.020402.

[25] I Šupić, A Coladangelo, R Augusiak, and A Acín, "Self-testing multipartite entangled states through projections onto two systems," **New Journal of Physics**, vol. 20, no. 8, 083041, Aug. 2018. [Online]. Available: https://doi.org/10.1088/1367-2630/aad89b.

[26] M. Fadel, **Self-testing dicke states**, 2017. [Online]. Available: https://arxiv.org/abs/1707.01215.

[27] X. Li, Y. Cai, Y. Han, Q. Wen, and V. Scarani, "Self-testing using only marginal information," **Phys. Rev. A**, vol. 98, 052331, 5 Nov. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.98.052331.

[28] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, "Robust self-testing of the three-qubit W state," **Phys. Rev. A**, vol. 90, 042339, 4 Oct. 2014. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.90.042339.

[29] K. F. Pál, T. Vértesi, and M. Navascués, "Device-independent tomography of multipartite quantum states," **Phys. Rev. A**, vol. 90, 042340, 4 Oct. 2014. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.90.042340.

[30] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, "Certifying the building blocks of quantum computers from *B*ell's theorem," **Phys. Rev. Lett.**, vol. 121, 180505, 18 Nov. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.121.180505.

[31] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, "Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems," **Quantum**, vol. 3, 198, Oct. 2019. [Online]. Available: https://doi.org/10.22331/q-2019-10-24-198.

[32] A. Coladangelo, K. Goh, and V. Scarani, "All pure bipartite entangled states can be self-tested," **Nat Commun**, vol. 8, 15485, 2017. [Online]. Available: https://doi.org/10.1038/ncomms15485.

[33] A. Coladangelo, "Generalization of the clauser-horne-shimony-holt inequality self-testing maximally entangled states of any local dimension," **Phys. Rev. A**, vol. 98, 052115, 5 Nov. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.98.052115.

[34] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, "Robust and versatile black-box certification of quantum devices," **Phys. Rev. Lett.**, vol. 113, 040401, 4 Jul. 2014. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.113.040401.

[35] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, "Physical characterization of quantum devices from nonlocal correlations," **Phys. Rev. A**, vol. 91, 022115, 2 Feb. 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.91.022115.

[36] D. M. Greenberger, M. A. Horne, and A. Zeilinger, **Going beyond bell's theorem**, 2021. arXiv: 0712.0921 [quant-ph]. [Online]. Available: https://doi.org/10.48550/arXiv.0712.0921.

[37] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, **npj Quantum Information**, vol. 7, 151, 2021. [Online]. Available: https://www.nature.com/articles/s41534-021-00490-3.

[38] S. Sarkar and R. Augusiak, "Self-testing of multipartite greenberger-horne-zeilinger states of arbitrary local dimension with arbitrary number of measurements per party," **Phys. Rev. A**, vol. 105, 032416, 3 Mar. 2022. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.105.032416.

[39] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, "Bell inequalities tailored to maximally entangled states," **Phys. Rev. Lett.**, vol. 119, 040402, 4 Jul. 2017. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.119.040402.

[40] R Augusiak, A Salavrakos, J Tura, and A Acín, "Bell inequalities tailored to the greenberger–horne–zeilinger states of arbitrary local dimension," **New Journal of Physics**, vol. 21, no. 11, 113001, Nov. 2019. [Online]. Available: https://doi.org/10.1088/1367-2630/ab4d9f.

[41] E. Woodhead, J. Kaniewski, B. Bourdoncle, **et al.**, "Maximal randomness from partially entangled states," **Phys. Rev. Research**, vol. 2, 042028, Jan. 2020. [Online]. Available: https://doi.org/10.1103/PhysRevResearch.2.042028.

[42] J. J. Borkała, C. Jebarathinam, S. Sarkar, and R. Augusiak, "Device-independent certification of maximal randomness from pure entangled two-qutrit states using non-projective measurements," **Entropy**, vol. 24, no. 3, 2022. [Online]. Available: https://www.mdpi.com/1099-4300/24/3/350.

[43] I. Šupić, D. Cavalcanti, and J. Bowles, "Device-independent certification of tensor products of quantum states using single-copy self-testing protocols," **Quantum**, vol. 5, 418, Mar. 2021. [Online]. Available: https://doi.org/10.22331/q-2021-03-23-418.

[44] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, "Self-testing of pauli observables for device-independent entanglement certification," **Phys. Rev. A**, vol. 98, 042336, 4 Oct. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.98.042336.

[45] M. McKague, "Self-testing in parallel with CHSH," **Quantum**, vol. 1, 1, Apr. 2017. [Online]. Available: https://doi.org/10.22331/q-2017-04-25-1.

[46] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, "Device-independent parallel self-testing of two singlets," **Phys. Rev. A**, vol. 93, 062121, 6 Jun. 2016. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.93.062121.

[47] J.-D. Bancal, N. Sangouard, and P. Sekatski, "Noise-resistant device-independent certification of bell state measurements," **Phys. Rev. Lett.**, vol. 121, 250506, 25 Dec. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.121.250506.

[48] M. O. Renou, J. Kaniewski, and N. Brunner, "Self-testing entangled measurements in quantum networks," **Phys. Rev. Lett.**, vol. 121, 250507, 25 Dec. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.121.250507.

[49] E. Schrödinger, "Discussion of probability relations between separated systems," **Math. Proc. Camb. Phil. Soc.**, vol. 31, no. 4, 555–563, Oct. 1935. [Online]. Available: https://doi.org/10.1017/s0305004100013554.

[50] H. M. Wiseman, S. J. Jones, and A. C. Doherty, "Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox," **Phys. Rev. Lett.**, vol. 98, 140402, 14 Apr. 2007. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.98.140402.

[51] I. Šupic and M. J. Hoban, "Self-testing through EPR-steering," **New J. Phys.**, vol. 18, no. 7, 075006, Jul. 2016. [Online]. Available: https://doi.org/10.1088/1367-2630/18/7/075006.

[52] A. Gheorghiu, P. Wallden, and E. Kashefi, "Rigidity of quantum steering and one-sided device-independent verifiable quantum computation," **New J. Phys.**, vol. 19, no. 2, 023043, Feb. 2017. [Online]. Available: https://doi.org/10.1088/1367-2630/aa5cff.

[53] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," **Phys. Rev. Lett.**, vol. 81, 3018–3021, 14 Oct. 1998. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.81.3018.

[54] D. Bruß and C. Macchiavello, "Optimal eavesdropping in cryptography with three-dimensional quantum states," **Phys. Rev. Lett.**, vol. 88, 127901, 12 Mar. 2002. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.88.127901.

[55] P. O. Boykin and V. Roychowdhury, "Optimal encryption of quantum bits," **Phys. Rev. A**, vol. 67, 042317, 4 Apr. 2003. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.67.042317.

[56] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," **Phys. Rev. A**, vol. 61, 062308, 6 May 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.61.062308.

[57] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," **Theoretical Computer Science**, vol. 560, 7–11, 2014, Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514004241.

[58] T. Durt and B. Nagler, "Covariant cloning machines for four-level systems," **Phys. Rev. A**, vol. 68, 042323, 4 Oct. 2003. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.68.042323.

[59] N. J. Cerf, "Pauli cloning of a quantum bit," **Phys. Rev. Lett.**, vol. 84, 4497–4500, 19 May 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.84.4497.

[60] N. Cerf, T. Durt, and N. Gisin, "Cloning a qutrit," **Journal of Modern Optics**, vol. 49, no. 8, 1355–1373, 2002. [Online]. Available: https://doi.org/10.1080/09500340110109043.

[61] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, "On mutually unbiased bases," **International Journal of Quantum Information**, vol. 08, no. 04, 535–640, 2010. [Online]. Available: https://doi.org/10.1142/S0219749910006502.

[62] S. Sarkar, D. Saha, and R. Augusiak, **Certification of incompatible measurements using quantum steering**, 2021. arXiv: 2107.02937 [quant-ph].

[63] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," **New Journal of Physics**, vol. 11, no. 4, 045021, Apr. 2009. [Online]. Available: https://doi.org/10.1088/1367-2630/11/4/045021.

[64] R. Colbeck and R. Renner, "Hidden variable models for quantum theory cannot have any local part," **Phys. Rev. Lett.**, vol. 101, 050403, 5 Aug. 2008. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.101.050403.

[65] S. Pironio, A. Acín, S. Massar, **et al.**, "Random numbers certified by Bell's theorem," **Nature**, vol. 464, no. 7291, 1021–1024, Apr. 2010. [Online]. Available: https://doi.org/10.1038/nature09008.

[66] S. Sarkar, J. J. Borkała, C. Jebarathinam, O. Makuta, D. Saha, and R. Augusiak, **Self-testing of any pure entangled state with minimal number of measurements and optimal randomness certification in one-sided device-independent scenario**, 2021. arXiv: 2110.15176 [quant-ph].

[67] R. F. Werner and M. M. Wolf, "Bound entangled gaussian states," **Phys. Rev. Lett.**, vol. 86, 3658–3661, 16 2001. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.86.3658.

[68] W. F. Stinespring, "Positive functions on $C*$-algebras," **Proc. Amer. Math. Soc.**, vol. 6, 211–216, 1955. [Online]. Available: https://doi.org/10.1090/S0002-9939-1955-0069403-4.

[69] F. S. Beckman and D. A. Quarles, "On isometries of euclidean spaces," **Proc. Amer. Math. Soc.**, vol. 4, 810–815, 1953. [Online]. Available: https://doi.org/10.1090/S0002-9939-1953-0058193-5.

[70] G. M. D'Ariano, P. L. Presti, and P. Perinotti, "Classical randomness in quantum measurements," **J. Phys. A: Math. Gen.**, vol. 38, no. 26, 5979–5991, Jun. 2005. [Online]. Available: https://doi.org/10.1088/0305-4470/38/26/010.

[71] P. Busch, P. Lahti, and R. F. Werner, "Colloquium: Quantum root-mean-square error and measurement uncertainty relations," **Rev. Mod. Phys.**, vol. 86, 1261–1281, 4 Dec. 2014. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.86.1261.

[72] O. Gühne, E. Haapasalo, T. Kraft, J.-P. Pellonpää, and R. Uola, **Incompatible measurements in quantum information science**, 2021. arXiv: 2112.06784 [quant-ph].

[73] V. Paulsen, "Completely bounded maps and operator algebras," Cambridge Studies in Advanced Mathematics, 2003. [Online]. Available: https://doi.org/10.1017/CBO9780511546631.

[74] J. Watrous, **The Theory of Quantum Information**. Cambridge University Press, 2018. [Online]. Available: https://doi.org/10.1017/9781316848142.

[75] J. S. Bell, "On the problem of hidden variables in quantum mechanics," **Rev. Mod. Phys.**, vol. 38, 447–452, 3 Jul. 1966. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.38.447.

[76] C. Bamps and S. Pironio, "Sum-of-squares decompositions for a family of clauser-horne-shimony-holt-like inequalities and their application to self-testing," **Phys. Rev. A**, vol. 91, 052111, 5 May 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.91.052111.

[77] B. S. Tsirel'son, "Quantum analogues of the Bell inequalities. the case of two spatially separated domains," **J Math Sci**, vol. 36, 557–570, 1987. [Online]. Available: https://doi.org/10.1007/BF01663472.

[78] S. Popescu and D. Rohrlich, "Quantum nonlocality as an axiom," **Found Phys**, vol. 24, 379–385, 1994. [Online]. Available: https://doi.org/10.1007/BF02058098.

[79] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," **Rev. Mod. Phys.**, vol. 86, 419–478, 2 Apr. 2014. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.86.419.

[80] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, "Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox," **Phys. Rev. A**, vol. 80, 032112, 3 Sep. 2009. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.80.032112.

[81] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, "Quantum steering," **Rev. Mod. Phys.**, vol. 92, 015001, 1 Mar. 2020. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.92.015001.

[82] R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication," **Phys. Rev. A**, vol. 56, 1201–1204, 2 Aug. 1997. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.56.1201.

[83] N. Herbert, "Cryptographic approach to hidden variables," **American Journal of Physics**, vol. 43, no. 4, 315–316, 1975. [Online]. Available: https://doi.org/10.1119/1.9861.

[84] A. K. Ekert, "Quantum cryptography based on Bell's theorem," **Phys. Rev. Lett.**, vol. 67, 661–663, 6 Aug. 1991. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.67.661.

[85] A. Acín, N. Gisin, and L. Masanes, "From Bell's theorem to secure quantum key distribution," **Phys. Rev. Lett.**, vol. 97, 120405, 12 Sep. 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.97.120405.

[86] A. Acín, S. Massar, and S. Pironio, "Efficient quantum key distribution secure against no-signalling eavesdroppers," **New Journal of Physics**, vol. 8, no. 8, 126–126, Aug. 2006. [Online]. Available: https://doi.org/10.1088/1367-2630/8/8/126.

[87] L. Masanes, "Universally composable privacy amplification from causality constraints," **Phys. Rev. Lett.**, vol. 102, 140501, 14 Apr. 2009. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.102.140501.

[88] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, "Full security of quantum key distribution from no-signaling constraints," **IEEE Transactions on Information Theory**, vol. 60, no. 8, 4973–4986, 2014. [Online]. Available: https://doi.org/10.1109/TIT.2014.2329417.

[89] L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices.," **Nat Commun**, vol. 2, no. 238, 2011. [Online]. Available: https://doi.org/10.1038/ncomms1244.

[90] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution," **Phys. Rev. Lett.**, vol. 95, 010503, 1 Jun. 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.95.010503.

[91] J. Barrett, R. Colbeck, and A. Kent, "Unconditionally secure device-independent quantum key distribution with only two devices," **Phys. Rev. A**, vol. 86, 062326, 6 Dec. 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.86.062326.

[92] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, "Secrecy extraction from no-signaling correlations," **Phys. Rev. A**, vol. 74, 042339, 4 Oct. 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.74.042339.

[93] E. Hänggi and R. Renner, **Device-independent quantum key distribution with commuting measurements**, 2010. [Online]. Available: https://arxiv.org/abs/1009.1833.

[94] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Méthot, and V. Scarani, "Testing the dimension of hilbert spaces," **Phys. Rev. Lett.**, vol. 100, 210503, 21 May 2008. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.100.210503.

[95] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, "Device-independent witnesses of genuine multipartite entanglement," **Phys. Rev. Lett.**, vol. 106, 250404, 25 Jun. 2011. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.106.250404.

[96] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, "Device-independent entanglement quantification and related applications," **Phys. Rev. Lett.**, vol. 111, 030501, 3 Jul. 2013. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.111.030501.

[97] K. T. Goh, C. Perumangatt, Z. X. Lee, A. Ling, and V. Scarani, "Experimental comparison of tomography and self-testing in certifying entanglement," **Phys. Rev. A**, vol. 100, 022305, 2 Aug. 2019. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.100.022305.

[98] R. Arnon-Friedman and J.-D. Bancal, "Device-independent certification of one-shot distillable entanglement," **New Journal of Physics**, vol. 21, no. 3, 033010, Mar. 2019. [Online]. Available: https://doi.org/10.1088/1367-2630/aafef6.

[99] A. Acín and L. Masanes, "Certified randomness in quantum physics," **Nature**, vol. 540, no. 7632, 213–219, Dec. 2016. [Online]. Available: https://doi.org/10.1038/nature20119.

[100] S. Pironio and S. Massar, "Security of practical private randomness generation," **Phys. Rev. A**, vol. 87, 012336, 1 Jan. 2013. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.87.012336.

[101] R. Colbeck and R. Renner, "No extension of quantum theory can have improved predictive power," **Nat Commun**, vol. 2, 411, 2011. [Online]. Available: https://doi.org/10.1038/ncomms1416.

[102] R. Colbeck and R. Renner, "Free randomness can be amplified," **Nature Phys**, vol. 8, 450–453, 2012. [Online]. Available: https://doi.org/10.1038/nphys2300.

[103] M. J. W. Hall, "Local deterministic model of singlet state correlations based on relaxing measurement independence," **Phys. Rev. Lett.**, vol. 105, 250404, 25 Dec. 2010. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.105.250404.

[104] R. Gallego **et al.**, "Full randomness from arbitrarily deterministic events," **Nat Commun**, vol. 4, 2654, 2013. [Online]. Available: https://doi.org/10.1038/ncomms3654.

[105] S. Fehr, R. Gelles, and C. Schaffner, "Security and composability of randomness expansion from Bell inequalities," **Phys. Rev. A**, vol. 87, 012335, 1 Jan. 2013. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.87.012335.

[106] D. E. Koh, M. J. W. Hall, Setiawan, **et al.**, "Effects of reduced measurement independence on Bell-based randomness expansion," **Phys. Rev. Lett.**, vol. 109, 160404, 16 Oct. 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.109.160404.

[107] S. Gómez, A. Mattar, I. Machuca, **et al.**, "Experimental investigation of partially entangled states for device-independent randomness generation and self-testing protocols," **Phys. Rev. A**, vol. 99, 032108, 3 Mar. 2019. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.99.032108.

[108] O. Andersson, P. Badziąg, I. Dumitru, and A. Cabello, "Device-independent certification of two bits of randomness from one entangled bit and gisin's elegant bell inequality," **Phys. Rev. A**, vol. 97, 012314, 1 Jan. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.97.012314.

[109] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín, "Unbounded randomness certification using sequences of measurements," **Phys. Rev. A**, vol. 95, 020102, 2 Feb. 2017. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.95.020102.

[110] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, "Optimal randomness certification from one entangled bit," **Phys. Rev. A**, vol. 93, 040102, 4 Apr. 2016. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.93.040102.

[111] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, "One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering," **Phys. Rev. A**, vol. 85, 010301, 1 Jan. 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.85.010301.

[112] E. Kaur, M. M. Wilde, and A. Winter, "Fundamental limits on key rates in device-independent quantum key distribution," **New Journal of Physics**, vol. 22, no. 2, 023039, Feb. 2020. [Online]. Available: http://dx.doi.org/10.1088/1367-2630/ab6eaa.

[113] K. Bartkiewicz, A. Černoch, K. Lemr, A. Miranowicz, and F. Nori, "Temporal steering and security of quantum key distribution with mutually unbiased bases against individual attacks," **Phys. Rev. A**, vol. 93, 062345, 6 Jun. 2016. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.93.062345.

[114] Y. Wang, W.-S. Bao, H.-W. Li, C. Zhou, and Y. Li, "Finite-key analysis for one-sided device-independent quantum key distribution," **Phys. Rev. A**, vol. 88, 052322, 5 Nov. 2013. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.88.052322.

[115] C. Zhou, P. Xu, W.-S. Bao, **et al.**, "Finite-key bound for semi-device-independent quantum key distribution," **Opt. Express**, vol. 25, no. 15, 16971–16980, Jul. 2017. [Online]. Available: http://opg.optica.org/oe/abstract.cfm?URI=oe-25-15-16971.

[116] T. Gehring **et al.**, "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," **Nat Commun**, vol. 6, 8795, 2015. [Online]. Available: https://doi.org/10.1038/ncomms9795.

[117] N. Walk, S. Hosseini, J. Geng, **et al.**, "Experimental demonstration of gaussian protocols for one-sided device-independent quantum key distribution," **Optica**, vol. 3, no. 6, 634–642, Jun. 2016. [Online]. Available: http://opg.optica.org/optica/abstract.cfm?URI=optica-3-6-634.

[118] Q. Y. He and M. D. Reid, "Genuine multipartite einstein-podolsky-rosen steering," **Phys. Rev. Lett.**, vol. 111, 250403, 25 Dec. 2013. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.111.250403.

[119] Y. Xiang, I. Kogias, G. Adesso, and Q. He, "Multipartite gaussian steering: Monogamy constraints and quantum cryptography applications," **Phys. Rev. A**, vol. 95, 010101, 1 Jan. 2017. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.95.010101.

[120] I. Kogias, P. Skrzypczyk, D. Cavalcanti, A. Acín, and G. Adesso, "Hierarchy of steering criteria based on moments for all bipartite quantum systems," **Phys. Rev. Lett.**, vol. 115, 210401, 21 Nov. 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.115.210401.

[121] I. Kogias, Y. Xiang, Q. He, and G. Adesso, "Unconditional security of entanglement-based continuous-variable quantum secret sharing," **Phys. Rev. A**, vol. 95, 012315, 1 Jan. 2017. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.95.012315.

[122] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, "Optimal randomness certification in the quantum steering and prepare-and-measure scenarios," **New Journal of Physics**, vol. 17, no. 11, 113010, Oct. 2015. [Online]. Available: https://doi.org/10.1088/1367-2630/17/11/113010.

[123] B. Coyle, M. J. Hoban, and E. Kashefi, "One-sided device-independent certification of unbounded random numbers," **Electronic Proceedings in Theoretical Computer Science**, vol. 273, 14–26, Jul. 2018. [Online]. Available: https://doi.org/10.4204%2Feptcs.273.2.

[124] P. Skrzypczyk and D. Cavalcanti, "Maximal randomness generation from steering inequality violations using qudits," **Phys. Rev. Lett.**, vol. 120, 260401, 26 Jun. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.120.260401.

[125] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, "Quantum randomness extraction for various levels of characterization of the devices," **Journal of Physics A: Mathematical and Theoretical**, vol. 47, no. 42, 424028, Oct. 2014. [Online]. Available: https://doi.org/10.1088/1751-8113/47/42/424028.

[126] M. Piani and J. Watrous, "Necessary and sufficient quantum information characterization of einstein-podolsky-rosen steering," **Phys. Rev. Lett.**, vol. 114, 060404, 6 Feb. 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.114.060404.

[127] R. Uola, T. Kraft, J. Shang, X.-D. Yu, and O. Gühne, "Quantifying quantum resources with conic programming," **Phys. Rev. Lett.**, vol. 122, 130404, 13 Apr. 2019. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.122.130404.

[128] S. Goswami, B. Bhattacharya, D. Das, S. Sasmal, C. Jebaratnam, and A. S. Majumdar, "One-sided device-independent self-testing of any pure two-qubit entangled state," **Phys. Rev. A**, vol. 98, 022311, 2 Aug. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.98.022311.

[129] H. Shrotriya, K. Bharti, and L.-C. Kwek, "Robust self testing of all pure bipartite maximally entangled states via quantum steering," **Phys. Rev. Research**, vol. 3, 033093, 2021. [Online]. Available: https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.3.033093.

[130] M. McKague and M. Mosca, "Generalized self-testing and the security of the 6-state protocol," **Theory of Quantum Computation, Communication, and Cryptography**, W. van Dam, V. M. Kendon, and S. Severini, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, 113–130.

[131] I. Šupić and J. Bowles, "Self-testing of quantum systems: A review," **Quantum**, vol. 4, 337, Sep. 2020. [Online]. Available: https://doi.org/10.22331/q-2020-09-30-337.

[132] K. T. Goh, J. Kaniewski, E. Wolfe, **et al.**, "Geometry of the set of quantum correlations," **Phys. Rev. A**, vol. 97, 022104, 2 Feb. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.97.022104.

[133] F. Baccari, R. Augusiak, I. Šupić, and A. Acín, "Device-independent certification of genuinely entangled subspaces," **Phys. Rev. Lett.**, vol. 125, 260507, 26 Dec. 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.125.260507.

[134] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, "Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems," **Quantum**, vol. 3, 198, Oct. 2019. [Online]. Available: https://doi.org/10.22331/q-2019-10-24-198.

[135] J. Kaniewski, "Weak form of self-testing," **Phys. Rev. Research**, vol. 2, 033420, 3 Sep. 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevResearch.2.033420.

[136] L. Masanes, "Asymptotic violation of bell inequalities and distillability," **Phys. Rev. Lett.**, vol. 97, 050503, 5 Aug. 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.97.050503.

[137] M. Navascués, S. Pironio, and A. Acín, "Bounding the set of quantum correlations," **Phys. Rev. Lett.**, vol. 98, 010401, 1 Jan. 2007. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.98.010401.

[138] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," **New Journal of Physics**, vol. 10, no. 7, 073013, Jul. 2008. [Online]. Available: https://doi.org/10.1088/1367-2630/10/7/073013.

[139] S. Pironio, M. Navascués, and A. Acín, "Convergent relaxations of polynomial optimization problems with noncommuting variables," **SIAM Journal on Optimization**, vol. 20, no. 5, 2157–2180, 2010. eprint: https://doi.org/10.1137/090760155. [Online]. Available: https://doi.org/10.1137/090760155.

[140] S.-L. Chen, H.-Y. Ku, W. Zhou, J. Tura, and Y.-N. Chen, "Robust self-testing of steerable quantum assemblages and its applications on device-independent quantum certification," **Quantum**, vol. 5, 552, 2021. [Online]. Available: https://quantum-journal.org/papers/q-2021-09-28-552/.

[141] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," **Communications of the ACM**, vol. 21, no. 2, 1978. [Online]. Available: https://doi.org/10.1145/359340.359342.

[142] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," **Proceedings 35th Annual Symposium on Foundations of Computer Science**, 1994, 124–134. [Online]. Available: https://doi.org/10.1109/SFCS.1994.365700.

[143] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," **IEEE Transactions on Information Theory**, vol. 55, no. 9, 4337–4347, 2009. [Online]. Available: https://ieeexplore.ieee.org/document/5208530.

[144] A. Acín, S. Massar, and S. Pironio, "Randomness versus nonlocality and entanglement," **Phys. Rev. Lett.**, vol. 108, 100402, 10 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.108.100402.

[145] O Nieto-Silleras, S Pironio, and J Silman, "Using complete measurement statistics for optimal device-independent randomness evaluation," **New Journal of Physics**, vol. 16, no. 1, 013035, Jan. 2014. [Online]. Available: https://doi.org/10.1088/1367-2630/16/1/013035.

[146] J.-D. Bancal, L. Sheridan, and V. Scarani, "More randomness from the same data," **New Journal of Physics**, vol. 16, no. 3, 033011, Mar. 2014. [Online]. Available: https://doi.org/10.1088/1367-2630/16/3/033011.

[147] I. Šupić, J. Bowles, M.-O. Renou, A. Acín, and M. J. Hoban, **Quantum networks self-test all entangled states**, 2022. [Online]. Available: https://arxiv.org/abs/2201.05032.

[148] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, "Bell inequalities for arbitrarily high-dimensional systems," **Phys. Rev. Lett.**, vol. 88, 040404, 4 Jan. 2002. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.88.040404.

[149] J. Barrett, A. Kent, and S. Pironio, "Maximally nonlocal and monogamous quantum correlations," **Phys. Rev. Lett.**, vol. 97, 170409, 17 Oct. 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.97.170409.

[150] M. Zukowski, A. Zeilinger, and M. A. Horne, "Realizable higher-dimensional two-particle entanglements via multiport beam splitters," **Phys. Rev. A**, vol. 55, 2564–2579, 4 Apr. 1997. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.55.2564.

[151] L. Aolita, R. Gallego, A. Cabello, and A. Acín, "Fully nonlocal, monogamous, and random genuinely multipartite quantum correlations," **Phys. Rev. Lett.**, vol. 108, 100401, 10 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.108.100401.

[152] G. Svetlichny, "Distinguishing three-body from two-body nonseparability by a bell-type inequality," **Phys. Rev. D**, vol. 35, 3066–3069, 10 May 1987. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevD.35.3066.

[153] J. Wang, S. Paesani, Y. Ding, **et al.**, "Multidimensional quantum entanglement with large-scale integrated optics," **Science**, vol. 360, no. 6386, 285–291, 2018. [Online]. Available: https://www.science.org/doi/abs/10.1126/science.aar7053.

[154] S. Beigi, "Separation of quantum, spatial quantum, and approximate quantum correlations," **Quantum**, vol. 5, 389, Jan. 2021. [Online]. Available: https://doi.org/10.22331/q-2021-01-28-389.

[155] H. Fu, "Constant-sized correlations are sufficient to self-test maximally entangled states with unbounded dimension," **Quantum**, vol. 6, 614, Jan. 2022. [Online]. Available: https://doi.org/10.22331/q-2022-01-03-614.

[156] L. Mančinska, J. Prakash, and C. Schafhauser, **Constant-sized robust self-tests for states and measurements of unbounded dimension**, 2021. [Online]. Available: https://arxiv.org/abs/2103.01729.

[157] F. Hirsch, M. T. Quintino, and N. Brunner, "Quantum measurement incompatibility does not imply Bell nonlocality," **Phys. Rev. A**, vol. 97, 012129, 1 Jan. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.97.012129.

[158] E. Bene and T. Vértesi, "Measurement incompatibility does not give rise to Bell violation in general," **New J. Phys.**, vol. 20, 013021, Jan. 2018. [Online]. Available: https://iopscience.iop.org/article/10.1088/1367-2630/aa9ca3.

[159] R. Uola, C. Budroni, O. Gühne, and J.-P. Pellonpää, "One-to-one mapping between steering and joint measurability problems," **Phys. Rev. Lett.**, vol. 115, 230402, 23 Dec. 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.115.230402.

[160] M. T. Quintino, T. Vértesi, and N. Brunner, "Joint measurability, einstein-podolsky-rosen steering, and Bell nonlocality," **Phys. Rev. Lett.**, vol. 113, 160402, 16 Oct. 2014. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.113.160402.

[161] D. Cavalcanti and P. Skrzypczyk, "Quantitative relations between measurement incompatibility, quantum steering, and nonlocality," **Phys. Rev. A**, vol. 93, 052112, 5 May 2016. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.93.052112.

[162] M. Marciniak, A. Rutkowski, Z. Yin, M. Horodecki, and R. Horodecki, "Unbounded violation of quantum steering inequalities," **Phys. Rev. Lett.**, vol. 115, 170401, 17 Oct. 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.115.170401.

[163] P. Skrzypczyk and D. Cavalcanti, "Loss-tolerant einstein-podolsky-rosen steering for arbitrary-dimensional states: Joint measurability and unbounded violations under losses," **Phys. Rev. A**, vol. 92, 022354, 2 Aug. 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.92.022354.

[164] S. Wollmann, R. Uola, and A. C. S. Costa, "Experimental demonstration of robust quantum steering," **Phys. Rev. Lett.**, vol. 125, 020404, 2 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.125.020404.

[165] M. M. Weston, S. Slussarenko, H. M. Chrzanowski, **et al.**, "Heralded quantum steering over a high-loss channel," **Science Advances**, vol. 4, no. 1, e1701230, 2018. [Online]. Available: https://www.science.org/doi/abs/10.1126/sciadv.1701230.

[166] P. Skrzypczyk and D. Cavalcanti, "Maximal randomness generation from steering inequality violations using qudits," **Phys. Rev. Lett.**, vol. 120, 260401, 26 Jun. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.120.260401.

[167] H. Sedrakyan and N. Sedrakyan, "Algebraic inequalities," in, Springer Nature, 2018. [Online]. Available: https://doi.org/10.1007/978-3-319-77836-5.

[168] "Heisenberg group and weyl operators," in **Symplectic Geometry and Quantum Mechanics**. Basel: Birkhäuser Basel, 2006, 159–193. [Online]. Available: https://doi.org/10.1007/3-7643-7575-2_6.

[169] A. Coladangelo, K. T. Goh, and V. Scarani, "All pure bipartite entangled states can be self-tested," **Nature Communications**, vol. 8, no. 1, 15485, May 2017. [Online]. Available: https://doi.org/10.1038/ncomms15485.

[170] A Tavakoli, M Farkas, D Rosset, J.-D. Bancal, and J. Kaniewski, "Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments," **Science Advances**, vol. 7, eabc3847, 7 2021. [Online]. Available: https://www.science.org/doi/10.1126/sciadv.abc3847.

Appendices

Appendix A

Some general mathematical facts

We prove here some identities that were extensively used throughout this work.

Fact 4. *Consider a matrix U acting on a Hilbert space $\mathscr{H}$ and $\overline{U} = \Pi U \Pi$, where Π is a projection onto some subspace $\mathscr{K}$ of $\mathscr{H}$. Then the following properties hold true:*

1. *If U is unitary, then $\overline{U}\overline{U}^\dagger \leq \mathbb{1}_{\mathscr{K}}$ where $\mathbb{1}_{\mathscr{K}}$ is identity acting on the subspace $\mathscr{K}$.*
2. *If U is hermitian, then $\overline{U}$ is also hermitian.*
3. *If both U and $\overline{U}$ are unitary, then $U = \overline{U} \oplus C$ such that C is also unitary.*

Proof. Given that $\overline{U}$ is a projection of U onto some subspace $\mathscr{K}$, then U can be written in the matrix form as

$$U = \begin{pmatrix} \overline{U} & A \\ B & C \end{pmatrix}, \tag{A.1}$$

where $A = \Pi U \Pi^\perp$, $B = \Pi^\perp U \Pi$, $C = \Pi^\perp U \Pi^\perp$. Here, $\Pi^\perp$ is the projection onto the subspace $\mathscr{K}^\perp$ of $\mathscr{H}$ that is orthogonal to $\mathscr{K}$. Since, U is unitary

$$UU^\dagger = \begin{pmatrix} \overline{U}\overline{U}^\dagger + AA^\dagger & \overline{U}B^\dagger + AC^\dagger \\ B\overline{U}^\dagger + CA^\dagger & BB^\dagger + CC^\dagger \end{pmatrix} = \begin{pmatrix} \mathbb{1}_{\mathscr{K}} & 0 \\ 0 & \mathbb{1}_{\mathscr{K}^\perp} \end{pmatrix}. \tag{A.2}$$

Here $\mathbb{1}_{\mathscr{K}^\perp}$ is identity acting on the subspace $\mathscr{K}^\perp$. Since $AA^\dagger$ is positive, we can conclude that

$$\overline{U}\overline{U}^\dagger \leq \mathbb{1}. \tag{A.3}$$

Now, if U is hermitian, that is, $U^\dagger = U$ then for $\overline{U}$ we have that

$$\overline{U}^\dagger = (\Pi U \Pi)^\dagger = \Pi U^\dagger \Pi = \Pi U \Pi = \overline{U} \tag{A.4}$$

and thus $\overline{U}$ is also hermitian if U is hermitian. One can also realise this by observing (A.1).

Let us now also assume that $\overline{U}$ is unitary, that is, $\overline{UU}^{\dagger} = \mathbb{1}$. Since U is unitary, from the diagonal element in (4.128) we have that $AA^{\dagger} = 0$ which implies that $A = 0$. Again, from the off-diagonal element, we have that $\overline{U}B^{\dagger} = 0$ which imposes that $B = 0$ as $\overline{U}$ is unitary and thus invertible. Similarly, one can prove that $C = 0$. Thus, the matrix U reduces to

$$U = \begin{pmatrix} \overline{U} & 0 \\ 0 & C \end{pmatrix} \tag{A.5}$$

which is equivalent to saying that $U = \overline{U} \oplus C$. □

Fact 5. *Consider two matrices R, Q acting on $d-$dimensional Hilbert space. Then, the following relation holds true when they act on the two-qudit maximally entangled state,*

$$R \otimes Q|\phi_d^+\rangle = RQ^T \otimes \mathbb{1}|\phi_d^+\rangle \tag{A.6}$$

such that Q^T represents the transpose of Q.

Proof. Let us first expand the matrices R, Q using the $d-$dimensional computational basis as

$$R = \sum_{i,j=0}^{d-1} r_{i,j}|i\rangle\langle j|, \qquad Q = \sum_{i,j=0}^{d-1} q_{i,j}|i\rangle\langle j|. \tag{A.7}$$

Let us now evaluate the right hand side of (A.6) by employing the form of the maximally entangled state $|\phi_d^+\rangle$ given in (4.16),

$$R \otimes Q|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i,k,j=0}^{d-1} r_{i,j} q_{k,j}|i\rangle|k\rangle. \tag{A.8}$$

Notice that $Q^T = \sum_{i,j=0}^{d-1} q_{j,i}|i\rangle\langle j|$ using which we get

$$RQ^T = \sum_{i,k,j=0}^{d-1} r_{i,j} q_{k,j}|i\rangle\langle k| \tag{A.9}$$

Now, using the above expression let us evaluate the left hand side of the equation (A.6)

$$RQ^T \otimes \mathbb{1}|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i,k,j=0}^{d-1} r_{i,j} q_{k,j}|i\rangle|k\rangle \tag{A.10}$$

which is exactly same as the left hand side (A.8). □

Fact 6. *The following identities hold true:*

$$\sum_{\substack{j=0\\ j\neq i}}^{d-1} \frac{1-\omega^{k(j-i)}}{1-\omega^{i-j}} = k, \qquad k=1,\dots,d-1, \qquad i=0,\dots,d-1, \tag{A.11}$$

and

$$\sum_{k=0}^{d-1} k\omega^{kn} = \frac{d}{\omega^n-1}, \qquad n=1,\dots,d-1. \tag{A.12}$$

Proof. Let us begin by proving the first identity (A.11). For this, we express the left-hand side of (A.11) as

$$\sum_{\substack{j=0\\ j\neq i}}^{d-1} \frac{1-\omega^{k(j-i)}}{1-\omega^{i-j}} = -\sum_{\substack{j=0\\ j\neq i}}^{d-1} \omega^{j-i}\left(\frac{1-\omega^{k(j-i)}}{1-\omega^{j-i}}\right). \tag{A.13}$$

Notice that the term appearing inside the bracket on the right-hand side of the above expression is a sum of a geometric sequence $\sum_{k=0}^{n-1} w^k = (1-w^n)/(1-w)$. Thus, the above expression can be rewritten as

$$\begin{aligned}\sum_{\substack{j=0\\ j\neq i}}^{d-1} \frac{1-\omega^{k(j-i)}}{1-\omega^{i-j}} &= -\sum_{\substack{j=0\\ j\neq i}}^{d-1}\left(\omega^{j-i}+\omega^{2(j-i)}+\ldots+\omega^{k(j-i)}\right)\\ &= -\sum_{n=1}^{k}\omega^{-ni}\left(\sum_{\substack{j=0\\ j\neq i}}^{d-1}\omega^{nj}\right).\end{aligned} \tag{A.14}$$

Evaluating the term inside the brackets of the above expression over x for any $n=1,\dots,d-1$, we obtain that

$$\sum_{\substack{j=0\\ j\neq i}}^{d-1}\omega^{nj} = \sum_{j=0}^{d-1}\omega^{nj} - \omega^{ni} = -\omega^{ni}, \tag{A.15}$$

where we used the fact that $\sum_{j=0}^{d-1}\omega^{nj} = \delta_{n,0}$. Plugging this last formula into Eq. (A.15) we finally arrive at Eq. (A.11).

Let us now prove the second identity (A.12) for which we again consider a geometric sum given by,

$$\sum_{k=0}^{d-1} x^k = \frac{1-x^d}{1-x}. \tag{A.16}$$

Now, we take the derivative of the above expression and then multiply the resultant equation with x on both sides, to finally obtain

$$\sum_{k=0}^{d-1} kx^k = x\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{1-x^d}{1-x}\right) = \frac{-dx^d}{1-x} + \frac{x(1-x^d)}{(1-x)^2} \ . \tag{A.17}$$

Substituting $x = \omega^n$ and using the fact that $\omega^d = 1$ we obtain (A.12). □

Appendix B

Proofs of some observations relevant to Chapter 3

Observation 3.1. *For any two unitary observables $A_{1,2}$ and $A_{1,3}$ related by the condition (3.57) which is given by*

$$\omega^{\frac{2k-d}{2m}} A_{1,2}^{k} A_{1,3}^{-k} + \omega^{-\frac{2k-d}{2m}} A_{1,3}^{k} A_{1,2}^{-k} = 2\cos\left(\frac{\pi}{m}\right) \mathbb{1}, \tag{B.1}$$

for $k = 1, 2, \ldots, d-1$. Then, the traces of $A_{1,2}$ and $A_{1,3}$ are related in the following way:

$$\mathrm{Tr}(A_{1,2}^{x}) = \omega^{\frac{2tx}{m}} \mathrm{Tr}\left(A_{1,2}^{(2t+1)x} A_{1,3}^{-2tx}\right). \tag{B.2}$$

for any non-negative integer $t \in \mathbb{N} \cup \{0\}$ and $x = 1, \ldots, \lfloor d/2 \rfloor$.

Proof. To prove the above claim we use the technique of mathematical induction. For this purpose, one can immediately observe that the condition (B.2) holds trivially for $t = 0$. Now, let us assume that the condition (B.2) is satisfied for $t = s-1$, that is,

$$\mathrm{Tr}(A_{1,2}^{x}) = \omega^{\frac{2(s-1)x}{m}} \mathrm{Tr}\left(A_{1,2}^{(2s-1)x} A_{1,3}^{-2(s-1)x}\right) \qquad x = 1, \ldots, \left\lfloor \frac{d}{2} \right\rfloor. \tag{B.3}$$

Let us now show that the condition (B.2) is also satisfied for $t = s$. For this purpose, let us consider (3.57) for $k = 2sx$ and multiply it with $A_{1,2}^{x}$ on both the sides. Now, taking the trace of the resultant expression yields,

$$\omega^{\frac{4sx-d}{2m}} \mathrm{Tr}\left(A_{1,2}^{(2s+1)x} A_{1,3}^{-2sx}\right) + \omega^{\frac{d-4sx}{2m}} \mathrm{Tr}\left(A_{1,3}^{2sx} A_{1,2}^{(-2s+1)x}\right) = \cos\left(\frac{\pi}{m}\right) \mathrm{Tr}\left(A_{1,2}^{x}\right). \tag{B.4}$$

Again, considering the condition (3.57) for $k = (2s-1)x$ but now we multiply it with $A_{1,3}^{x}$

on both the sides. Taking the trace of the resulting expression gives us,

$$\omega^{\frac{2(2s-1)x-d}{2m}}\mathrm{Tr}\left(A_{1,2}^{(2s-1)x}A_{1,3}^{-2(s-1)x}\right)+\omega^{\frac{d-2(2s-1)x}{2m}}\mathrm{Tr}\left(A_{1,3}^{2sx}A_{1,2}^{(-2s+1)x}\right)=\cos\left(\frac{\pi}{m}\right)\mathrm{Tr}\left(A_{1,3}^{x}\right). \tag{B.5}$$

Utilising the condition (3.64) for $k=x$, the above expression simplifies to

$$\omega^{\frac{4(s-1)x-d}{2m}}\mathrm{Tr}\left(A_{1,2}^{(2s-1)x}A_{1,3}^{-2(s-1)x}\right)+\omega^{\frac{d-4sx}{2m}}\mathrm{Tr}\left(A_{1,3}^{2sx}A_{1,2}^{(-2s+1)x}\right)=\cos\left(\frac{\pi}{m}\right)\mathrm{Tr}\left(A_{1,2}^{x}\right), \tag{B.6}$$

for $x=1,\ldots,\lfloor d/2\rfloor$ where $\lfloor d/2\rfloor$ denotes the largest integer smaller than $d/2$. Finally, subtracting Eq. (B.6) from Eq. (B.4) we obtain

$$\mathrm{Tr}\left(A_{1,2}^{(2s+1)x}A_{1,3}^{-2sx}\right)=\omega^{-\frac{2x}{m}}\left(A_{1,2}^{(2s-1)x}A_{1,3}^{-2(s-1)x}\right), \tag{B.7}$$

which along with Eq. (B.3) gives us the desired result,

$$\mathrm{Tr}\left(A_{1,2}^{(2s+1)x}A_{1,3}^{-2sx}\right)=\omega^{-\frac{2sx}{m}}\mathrm{Tr}(A_{1,2}^{x}). \tag{B.8}$$

□

Observation 3.2. *Consider two unitary observables $A_{1,2}$ and $A_{1,3}$ related by the condition (3.71) which is given by*

$$A_{1,3}^{k}=-(k-1)\omega^{\frac{k}{m}}A_{1,2}^{k}+\omega^{\frac{k-1}{m}}\sum_{t=0}^{k-1}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-1-t} \tag{B.9}$$

for any $k=1,\ldots,d-1$ and $m\geq 2$. If $A_{1,2}=Z_d\otimes\mathbb{1}$ and $A_{1,3}=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes F_{ij}$, then the matrices F_{ij} are related as:

$$\begin{aligned}-(k-1)\sum_{i,j=0}^{d-1}\omega^{ki}|i\rangle\langle j|\otimes F_{ij}+\omega^{-\frac{1}{m}}\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes\left[\sum_{\substack{l=0\\ l\neq i}}^{d-1}\left(\frac{\omega^{ki}-\omega^{kl}}{\omega^{i}-\omega^{l}}\right)F_{il}F_{lj}+k\omega^{(k-1)i}F_{ii}F_{ij}\right]\\ =-k\omega^{\frac{1}{m}}\sum_{i=0}^{d-1}\omega^{(k+1)i}|i\rangle\langle i|\otimes\mathbb{1}+\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes\sum_{t=0}^{k}\omega^{kj+t(i-j)}F_{ij}.\end{aligned} \tag{B.10}$$

for any $k=1,\ldots,d-1$ and $m\geq 2$.

Proof. To begin the proof, let us first notice that $A_{1,3}^{k+1}=A_{1,3}^{k}A_{1,3}$. Now, plugging in $A_{1,3}^{k+1}$

and $A_{1,3}^k$ using Eq. (3.71) gives us,

$$-k\omega^{\frac{1}{m}}A_{1,2}^{k+1}+\sum_{t=0}^{k}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-t}=-(k-1)A_{1,2}^{k}A_{1,3}+\omega^{-\frac{1}{m}}\sum_{t=0}^{k-1}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-1-t}A_{1,3}. \tag{B.11}$$

Substituting the explicit forms of the observables $A_{1,2}=Z_d\otimes\mathbb{1}$ and $A_{1,3}=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes F_{ij}$, we obtain that

$$\sum_{t=0}^{k-1}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-1-t}A_{1,3}=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes\sum_{l=0}^{d-1}\sum_{t=0}^{k-1}\omega^{l(k-1)}\omega^{t(i-l)}F_{il}F_{lj}. \tag{B.12}$$

Splitting the sum over l appearing on the right hand side into two parts: $l=i$ and $l\neq i$, and then using the sum computed using the geometric series

$$\sum_{t=0}^{k-1}\omega^{t(i-l)}=\frac{1-\omega^{k(i-l)}}{1-\omega^{i-l}}, \tag{B.13}$$

we obtain that

$$\sum_{t=0}^{k-1}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-1-t}A_{1,3}=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes\left[\sum_{\substack{l=0\\l\neq i}}^{d-1}\left(\frac{\omega^{ki}-\omega^{kl}}{\omega^{i}-\omega^{l}}\right)F_{il}F_{lj}+k\omega^{(k-1)i}F_{ii}F_{ij}\right]. \tag{B.14}$$

Using exactly the same technique, the sum on the left-hand side of Eq. (B.11) can be rewritten as,

$$\sum_{t=0}^{k}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-t}=\sum_{i,j=0}^{d-1}\omega^{kj}\sum_{t=0}^{k}\omega^{t(i-j)}|i\rangle\langle j|\otimes F_{ij}. \tag{B.15}$$

Finally substituting Eqs. (B.14) and (B.15) into Eq. (B.11), we obtain (3.87). □

Observation 3.3. *Consider the following unitary operators* $W_1,W_2,W_{\text{odd}},W_{\text{ev}}:\mathbb{C}^d\to\mathbb{C}^d$ *given by*

$$\begin{aligned}
W_1 &= \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{3i}{2m}+ij+\frac{j}{2}}|i\rangle\langle j|,\\
W_2 &= \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{2i}{m}+ij+\frac{j}{2}}|d-1-i\rangle\langle j|,\\
W_{\text{odd}} &= \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{i}{m}+ij+\frac{j}{2}}|i\rangle\langle j|,\\
W_{\text{ev}} &= \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{i}{m}+ij+\frac{j}{2}}|d-1-i\rangle\langle j|,
\end{aligned} \tag{B.16}$$

where $\{|i\rangle\}$ is the standard basis on $\mathbb{C}^d$. These unitaries transform $Z_d, T_{d,m}$ as defined in Eq. (3.32) to the ideal measurements given in Eq. (3.11),(3.12) and (3.13) in the following way: $\mathscr{O}_{i,2} = W_i Z_d W_i^\dagger$ and $\mathscr{O}_{i,3} = W_i T_{d,m} W_i^\dagger$ for the parties $i = 1,2$, and $\mathscr{O}_{n_{\text{odd}},2} = W_{\text{odd}} Z_d W_{\text{odd}}^\dagger, \mathscr{O}_{n_{\text{odd}},3} = W_{\text{odd}} T_{d,m} W_{\text{odd}}^\dagger$, and $\mathscr{O}_{n_{\text{ev}},2} = W_{\text{ev}} Z_d W_{\text{ev}}^\dagger, \mathscr{O}_{n_{\text{ev}},3} = W_{\text{ev}} T_{d,m} W_{\text{ev}}^\dagger$ for remaining parties. Here, the subscripts odd and ev refer to parties that are numbered by odd and even numbers respectively.

Proof. Before proceeding, let us recall the measurements $Z_d, T_{d,m}$ as defined in Eq. (3.32)

$$\begin{aligned} Z_d &= \sum_{i=0}^{d-1} \omega^i |i\rangle\langle i| \\ T_{d,m} &= \sum_{i=0}^{d-1} \omega^{i+\frac{1}{m}} |i\rangle\langle i| - \frac{2\mathbb{i}}{d} \sin\left(\frac{\pi}{m}\right) \sum_{i,j=0}^{d-1} (-1)^{\delta_{i,0}+\delta_{j,0}} \omega^{\frac{i+j}{2}-\frac{d-2}{2m}} |i\rangle\langle j|. \end{aligned} \tag{B.17}$$

Let us also recall the ideal observables given in Eq. (3.11),(3.12) and (3.13) which we express here in their matrix form as

$$\begin{aligned} \mathscr{O}_{1,x} &= \sum_{i=0}^{d-2} \omega^{\gamma_m(\alpha)} |i\rangle\langle i+1| + \omega^{(1-d)\gamma_m(\alpha)} |d-1\rangle\langle 0|, \\ \mathscr{O}_{2,x} &= \sum_{i=0}^{d-2} \omega^{\zeta_m(\alpha)} |i+1\rangle\langle i| + \omega^{(1-d)\zeta_m(\alpha)} |0\rangle\langle d-1| \end{aligned} \tag{B.18}$$

for the first two parties, and

$$\begin{aligned} \mathscr{O}_{\text{odd},x} &= \sum_{i=0}^{d-2} \omega^{\theta_m(\alpha)} |i\rangle\langle i+1| + \omega^{(1-d)\theta_m(\alpha)} |d-1\rangle\langle 0|, \\ \mathscr{O}_{\text{ev},x} &= \sum_{i=0}^{d-2} \omega^{\theta_m(\alpha)} |i+1\rangle\langle i| + \omega^{(1-d)\theta_m(\alpha)} |0\rangle\langle d-1| \end{aligned} \tag{B.19}$$

for the remaining parties. Let us begin by finding the eigen-decomposition of the ideal measurements (3.11),(3.12) and (3.13) for the second and third measurements for each party as,

$$\mathscr{O}_{n,x} = \sum_{r=0}^{d-1} \omega^r |r\rangle\langle r|_{n,x} \tag{B.20}$$

with $x = 2,3$ and $n = 1,2,\ldots,N$, where the eigenvectors are defined as

$$\begin{aligned} |r\rangle_{1,x} &= \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \omega^{(r-\gamma_m(x))q} |q\rangle, \\ |r\rangle_{2,x} &= \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \omega^{-(r-\zeta_m(x))q} |q\rangle, \\ |r\rangle_{n_{\text{odd}},x} &= \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \omega^{(r-\theta_m(x))q} |q\rangle, \\ |r\rangle_{n_{\text{ev}},x} &= \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \omega^{-(r-\theta_m(x))q} |q\rangle \end{aligned} \tag{B.21}$$

where the coefficients $\gamma_m(x)$, $\zeta_m(x)$ and $\theta_m(x)$ are given in Eq. (3.16) and $\{|q\rangle\}$ denotes the computational basis of $\mathbb{C}^d$. Notice that the set of vectors $\{|r\rangle_{i,x}\}$ for any particular i and x are mutually orthogonal.

Let us now consider the eigen-decompositions of Z_d and $T_{d,m}$,

$$Z_d = \sum_{q=0}^{d-1} \omega^q |q\rangle\langle q|, \qquad T_{d,m} = \sum_{r=0}^{d-1} \omega^r |r\rangle\langle r|_T. \tag{B.22}$$

Here again $\{|q\rangle\}$ is the computational basis of $\mathbb{C}^d$ and $|r\rangle_T$ denote the eigenvectors of $T_{d,m}$ given by

$$|r\rangle_T = \frac{2\mathbb{i}}{d} \sin\left(\frac{\pi}{m}\right) \omega^{-\frac{d}{2m}} \sum_{q=0}^{d-1} (-1)^{\delta_{q,0}} \frac{\omega^{-\frac{q}{2}}}{1-\omega^{r-q-\frac{1}{m}}} |q\rangle. \tag{B.23}$$

Let us now go back to the main proof and show that the unitaries $W_1, W_2, W_{\text{odd}}, W_{\text{ev}}$ (B.16) transform Z_d and $T_{d,m}$ to the ideal measurements $\mathscr{O}_{i,2}$ and $\mathscr{O}_{i,3}$ for any $i = 1,2,\ldots,N$. For this purpose, we show that under the action of the unitaries the eigenvectors of one observable transform to the eigenvectors of another observable up to a complex number.

Let us begin by considering the first party. The action of $W_1^\dagger$ on the eigenvectors of $\mathscr{O}_{1,2}$, $|r\rangle_{1,2}$, given explicitly in Eq. (B.21) can be expressed as

$$W_1^\dagger |r\rangle_{1,2} = \frac{1}{d} \sum_{j,q=0}^{d-1} (-1)^{\delta_{j,0}} \omega^{(r-j)q} \omega^{-\frac{j}{2}} |j\rangle. \tag{B.24}$$

Using the fact that $\sum_{q=0}^{d-1} \omega^{(r-j)q} = d\delta_{r,j}$, the above expression simplifies to

$$W_1^\dagger |r\rangle_{1,2} = \omega^{\delta_{j,0} - \frac{j}{2}} |j\rangle. \tag{B.25}$$

Recall that $|j\rangle$ are the eigenvectors of Z_d and thus we obtain that $W_1^\dagger \mathscr{O}_{1,2} W_1 = Z_d$. Now, the action of $W_1^\dagger$ on the eigenvectors of $\mathscr{O}_{1,3}$, $|r\rangle_{1,3}$, given explicitly in Eq. (B.21) can be expressed as

$$W_1^\dagger |r\rangle_{1,3} = \frac{1}{d} \sum_{j,q=0}^{d-1} (-1)^{\delta_{j,0}} \omega^{(r-j-\frac{1}{m})q} \omega^{-\frac{j}{2}} |j\rangle. \tag{B.26}$$

Using the following relation derived from the sum of a geometric series

$$\sum_{l=0}^{d-1} \omega^{(r-k-\frac{1}{m})l} = \frac{1-\omega^{-\frac{d}{m}}}{1-\omega^{r-k-\frac{1}{m}}} = 2\mathbb{i} \sin\left(\frac{\pi}{m}\right) \frac{\omega^{-\frac{d}{2m}}}{1-\omega^{r-k-\frac{1}{m}}}, \tag{B.27}$$

and (B.23), the expression (B.26) simplifies to

$$\begin{aligned} W_1^\dagger |r\rangle_{1,3} &= \frac{2\mathbb{i}}{d} \sin\left(\frac{\pi}{m}\right) \omega^{-\frac{d}{2m}} \sum_{j=0}^{d-1} (-1)^{\delta_{j,0}} \frac{\omega^{-\frac{j}{2}}}{1-\omega^{r-j-\frac{1}{m}}} |j\rangle \\ &= |r\rangle_{T_{d,m}}. \end{aligned} \tag{B.28}$$

As a consequence, $W_1^\dagger \mathscr{O}_{1,3} W_1 = T_{d,m}$.

Let us now consider the second party. The action of $W_2^\dagger$ on the eigenvectors of $\mathscr{O}_{2,2}$, $|r\rangle_{2,2}$, given explicitly in Eq. (B.21) can be expressed as

$$W_2^\dagger |r\rangle_{2,2} = \frac{1}{d} \sum_{j,q=0}^{d-1} (-1)^{\delta_{j,0}} \omega^{(r-j)q + (d-1)\left(\frac{2}{m}-r\right) - \frac{j}{2}} |j\rangle, \tag{B.29}$$

and, after employing the fact that $\sum_{q=0}^{d-1} \omega^{(r-j)q} = d\delta_{r,j}$, the above expression simplifies to

$$W_2^\dagger |r\rangle_{2,2} = (-1)^{\delta_{j,0}} \omega^{(d-1)\left(\frac{2}{m}-j\right) - \frac{j}{2}} |j\rangle. \tag{B.30}$$

Recall that $|j\rangle$ are the eigenvectors of Z_d and thus we obtain that $W_2^\dagger \mathscr{O}_{2,2} W_2 = Z_d$. Now, the action of $W_2^\dagger$ on the eigenvectors of $\mathscr{O}_{2,3}$, $|r\rangle_{2,3}$, given explicitly in Eq. (B.21) can be expressed as

$$W_2^\dagger |r\rangle_{2,3} = \frac{1}{d} \sum_{j,q=0}^{d-1} (-1)^{\delta_{j,0}} \omega^{(r-j-\frac{1}{m})q + (d-1)\left(\frac{2}{m}-r\right) - \frac{j}{2}} |j\rangle, \tag{B.31}$$

which can be simplified using Eq. (B.27) to

$$W_2^\dagger |r\rangle_{2,3} = \omega^{(d-1)\left(\frac{2}{m}-r\right)} |r\rangle_T. \tag{B.32}$$

As a consequence, $W_2^\dagger \mathscr{O}_{2,3} W_1 = T_{d,m}$. Let us now consider the parties indexed by odd numbers. The action of $W_{\text{odd}}^\dagger$ on the eigenvectors of $\mathscr{O}_{n_{odd},2}$, $|r\rangle_{n_{odd},2}$, given explicitly in Eq. (B.21) can be expressed as

$$W_{\text{odd}}^\dagger |r\rangle_{n_{\text{odd}},2} = \frac{1}{d} \sum_{j,q=0}^{d-1} (-1)^{\delta_{j,0}} \omega^{(r-j)q} \omega^{-\frac{j}{2}} |j\rangle, \tag{B.33}$$

which by again employing the fact that $\sum_{q=0}^{d-1} \omega^{(r-j)q} = d\delta_{r,j}$, simplifies to

$$W_{\text{odd}}^\dagger |r\rangle_{\text{odd},2} = (-1)^{\delta_{j,0}} \omega^{-j/2} |j\rangle. \tag{B.34}$$

Analogously for $\mathscr{O}_{\text{odd},3}$, we have that

$$W_{\text{odd}}^\dagger |r\rangle_{\text{odd},3} = \frac{1}{d} \sum_{j,q=0}^{d-1} (-1)^{\delta_{j,0}} \omega^{(r-j-\frac{1}{m})q} \omega^{-\frac{j}{2}} |j\rangle. \tag{B.35}$$

which by again utilising the sum (B.27) simplifies to

$$W_{\text{odd}}^\dagger |r\rangle_{\text{odd},3} = |r\rangle_T. \tag{B.36}$$

As a consequence, $W_{\text{odd}}^\dagger \mathscr{O}_{\text{odd},3} W_{\text{odd}} = T_{d,m}$. Let us finally consider the parties indexed by even numbers. The action of $W_{\text{ev}}^\dagger$ on the eigenvectors of $\mathscr{O}_{n_{ev},2}$, $|r\rangle_{n_{ev},2}$, given explicitly in Eq. (B.21) can be expressed as

$$W_{\text{ev}}^\dagger |r\rangle_{\text{ev},2} = \frac{1}{d} \sum_{j,q=0}^{d-1} (-1)^{\delta_{j,0}} \omega^{(r-j)q + (d-1)\left(\frac{2}{m}-r\right) - \frac{j}{2}} |j\rangle, \tag{B.37}$$

which by again employing the fact that $\sum_{q=0}^{d-1} \omega^{(r-j)q} = d\delta_{r,j}$, simplifies to

$$W_{\text{ev}}^\dagger |r\rangle_{\text{ev},2} = (-1)^{\delta_{r,0}} \omega^{(d-1)\left(\frac{2}{m}-r\right) - \frac{r}{2}} |r\rangle. \tag{B.38}$$

As a consequence, $W_{\text{ev}}^\dagger \mathscr{O}_{\text{ev},2} W_{\text{ev}} = Z_d$. Analogously for $\mathscr{O}_{\text{ev},3}$, we have that

$$W_{\text{ev}}^\dagger |r\rangle_{\text{ev},3} = \frac{1}{d} \sum_{j,q=0}^{d-1} (-1)^{\delta_{j,0}} \omega^{(r-j-\frac{1}{m})q + (d-1)\left(\frac{2}{m}-r\right) - \frac{j}{2}} |j\rangle, \tag{B.39}$$

which by employing the sum (B.27), simplifies to

$$W_{\text{ev}}^\dagger |r\rangle_{\text{ev},3} = \omega^{(d-1)\left(\frac{2}{m}-r\right)} |r\rangle_T. \tag{B.40}$$

As a consequence, $W_{\text{ev}}^\dagger \mathscr{O}_{\text{ev},3} W_{\text{ev}} = T_{d,m}$. □

Appendix C

Proofs of some observations relevant to Chapter 5

Observation 5.1. *The matrix*

$$\tilde{Z} = \overline{Z}_A + \gamma(\boldsymbol{\alpha})\mathbb{1} = [1+\gamma(\boldsymbol{\alpha})]\mathbb{1} - \sum_{k=1}^{d-1} \delta_k(\boldsymbol{\alpha}) Z_d^k \tag{C.1}$$

with γ and δ_k defined in Eq. (5.2) is positive and invertible.

Proof. Let us first observe that that the above matrix (C.1) is diagonal in the computational basis as well as hermitian which stems from the fact that $\delta_k^* = \delta_{d-k}$ and that $Z_d^\dagger = Z_d^{d-k}$. To show that this matrix is positive and invertible, we compute its eigenvalues and show that they are strictly positive. For this purpose, we plug in the explicit form of δ_k and evaluate its diagonal elements in the computational basis as

$$\lambda_l = 1 + \gamma(\boldsymbol{\alpha}) + \frac{\gamma(\boldsymbol{\alpha})}{d} \sum_{k=1}^{d-1} \sum_{\substack{i,j=0 \\ i\neq j}}^{d-1} \frac{\alpha_i}{\alpha_j} \omega^{k(l-j)} \quad \text{for} \quad l = 0,\ldots,d-1, \tag{C.2}$$

such $\tilde{Z} = \sum_l \lambda_l |l\rangle\langle l|$. After simple manipulations and rearrangements, the above expression simplifies to

$$\lambda_l = \frac{\gamma(\boldsymbol{\alpha})}{\alpha_l} \sum_{i=0}^{d-1} \alpha_i. \tag{C.3}$$

Let us note that $\gamma(\boldsymbol{\alpha})$ and α_i's are strictly positive for all i's. Thus, we can conclude that all the eigenvalues of the matrix (C.1) are positive and as a consequence the matrix (C.1) is invertible. □

Observation 5.2. *Let us consider that the elements of two POVM's* $\{\mathscr{I}_b\}$ *and* $\{R_b\}$ *are related as*

$$\mathscr{I}_b \geq \pm \mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right], \tag{C.4}$$

such that $L^a_{B''}$ *is a matrix given in* (5.111) *and* $\{\mathscr{I}_b\}$ *is an extremal rank-one POVM. Then,*

$$\mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right] = \lambda'_b |\mu_b\rangle\langle\mu_b|. \tag{C.5}$$

Proof. As the POVM $\{\mathscr{I}_b\}$ is extremal and of rank-one, we can express each of its elements as $\mathscr{I}_b = \lambda_b |\mu_b\rangle\langle\mu_b|$ for all b. Choosing a particular b and the corresponding vector $|\mu_b\rangle$, we can construct an orthonormal basis $\{|\phi_i\rangle\}$ with $i = 0, \ldots, d-1$ such that $|\phi_0\rangle = |\mu_b\rangle$. Now, multiplying the above inequality (C.4) with $\langle\phi_j|$ from left and $|\phi_i\rangle$ from right hand side, we arrive at

$$\forall_{i,j} \qquad \langle\phi_j|\mathscr{I}_b|\phi_i\rangle \geq \pm\langle\phi_j|\mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right]|\phi_i\rangle. \tag{C.6}$$

For $i \neq 0$ or $j \neq 0$ the above expression yields

$$0 \geq \pm\langle\phi_j|\mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right]|\phi_i\rangle, \tag{C.7}$$

which is only possible if $\langle\phi_j|\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right]|\phi_i\rangle = 0$ for any $i \neq 0$ or $j \neq 0$ and thus we can straightforwardly conclude Eq. (C.5). Moreover, for $i = j = 0$, Eq. (C.6) gives

$$\lambda_b \geq \pm\langle\mu_b|\mathrm{Tr}_{B''}\left[(\mathbb{1}_{B'} \otimes L^a_{B''})R_b\right]|\mu_b\rangle, \tag{C.8}$$

which additionally imposes that $\lambda_b \geq \pm\lambda'_b$. □