Device-independent certification of quantum resources

The Institute of Photonic Sciences

Ivan Šupić

July 16, 2018

Acknowledgements

At the end of my PhD I feel incredibly blessed and happy for the last years spent in Barcelona. It has been a period of a big professional and personal growth for me and I am deeply grateful to many people who helped me to be where I am now.

First and foremost I owe big gratitude to Toni Acin for letting me do my master thesis and PhD in his group. You have created a great atmosphere in the group for Quantum Information Theory which made my PhD journey very pleasant and exciting. I am grateful for mentoring but also giving me freedom to do research I like and enjoy, for sharing your ideas and thoughts and giving many valuable advices.

No less gratitude I owe to my co-supervisor and office mate Dani Cavalcanti. Thanks for helping me grow as a reseracher and involving me in our beautiful projects about teleportation.

I was very lucky to work with some amazing people in QIT group and also learn a lot from them. Huge thanks to Matty Hoban, my master thesis supervisor, who introduced me to the field of quantum nonlocality, supervised my first steps as a researcher and continued to be a wonderful collaborator during my PhD. A warm thanks to Paul, for his patience and kindness and for teaching me so much about so many different topics. I owe immense gratitude to Remik, for helping me with my first project during PhD and continuing working with me, i.e. teaching me how to solve problems and write papers. Many thanks to Joe for a great project we managed to finish together and for being a true inspiration as a scientist. Also, I have to thank to Janek, for sharing his excitement about science and showing me how to patiently and systematically attack difficult problems. Furthermore, I was happy to work with my fellow young PhD students Alexia, Boris, Flavio, Flo and Leo. We were learning many things together and without them this thesis would never be finished. Many thanks to the rest of my collaborators Andrea, Jed and Jordi. I hope we will continue solving interesting problems.

QIT group is a great PhD environment. I met so many wonderful people during my master and PhD. A huge thanks to: Alejandro, Alex, Ariel, Arnau, Belen, Bogna, Christian, Chung-Yun, Dario, Elsa, Eric, Erik, Felix, Gabriel, Gonzalo, Jimmy, Karen, Maciek, Mafalda, Manuel, Markus, Marti, Matteo, Michal, Moha, Patrick, Peter, Senaida, Victoria, Xavier, Zahra.

I would like to thank to Thomas Vidick for letting me spend three months in his group in Caltech and discussing science with me. It was a complete perspective-changing period for me.

I owe special gratitude to several people who left a huge mark on my life in Barcelona, made me feel like at home and influenced my significant personal growth. A paragraph in this acknowledgments cannot do any justice to all goods I received from Alexia, Boris, Flavio, Leo, Joe, Sarah and Simona. Special thanks for Antoine and Maria! I hope for a lifetime of happy encounters with them.

For reading parts of this thesis and giving a valuable feedback I thank Alexia, Boris, Flavio, Joe, Marijana and Sarah.

Tokom doktorata sam se često i rado vraćao dobrom starom Beogradu da napunim baterije. Tamo su me uvijek rado dočekivali Aco i Zdenka i hvala im na svemu. Za radosno prijateljstvo i nesebičnu pomoć hvala Vesni i divnoj duhovnoj tvrdjavi – svetoarhangelskoj zajednici u Zemunu.

U mojoj Crnoj Gori sam uvijek nalazio neophodnu podršku i inspiraciju. Veliku blagodarnost dugujem ocu Bobanu za strpljenje i korisne savjete. Hvala Andjeli, Antoniju, Stevu, Vesni i Zelu na svim radosnim susretima.

Ogromnu inspiraciju za svoj naučni rad crpim iz prijateljstva sa Nenom, Ivankom i Jelicom. Hvala im za sva divna druženja.

Svakako da ne bih uspio ni jedan korak napraviti bez bezuslovne i neiscrpne ljubavi i podrške moje porodice. Hvala stricu Bogdanu za sve srdačne razgovore. Neizmjerno hvala stricu Petru i strini Gojki za i moralnu i materijalnu podršku i pažnju svih ovih godina. Najveće radosno hvala Anji, Davidu i Juliji i mojim sestrama Snežani, Branki i Veri što su uvijek tu za mene. Mojoj majki Mileni hvala za ispunjavanje svih mojih želja i potreba tokom čitavog školovanja. Ona je najzaslužnija što sam stigao dovde.

Abstract

The last two decades have been a very fruitful period for the fundamental research related to quantum information theory. Today we have a fairly good understanding of how intrinsically quantum properties affect various computational and cryptographic tasks. Practical implementations are advancing as well. Devices performing quantum key distribution or quantum random number generation are already commercially available. As time goes more resources are being invested in building a device which would demonstrate and exploit quantum computational supremacy. In the context of the impending second quantum revolution it is of crucial importance to build new certification tools, improve the existing ones and understand their limits. When assessing the non-classicality of a given device it is essential to estimate which assumptions about the device are not jeopardizing the certification procedure. *Device-independent* scenario does not make any assumptions about the inner functioning of devices, but usually only assumes the correctness of quantum theory. It gained a lot of attention because it manages to certify the quantum character of certain devices while giving to potential adversaries all power allowed by the laws of physics. Device-independent certification of various quantum resources is the main subject of this thesis.

In the first part of the thesis we focus on self-testing, one of the simplest device-independent protocols. It aims to recover quantum states solely from the observed measurement correlations. It has a fundamental importance for the device-independent paradigm because it shows which quantum states can leave a device-independent 'imprint'. Practically, it bears a significance as a possible first step in more complex protocols such as blind quantum computing, randomness generation or quantum key distribution. In this thesis we present several new self-testing results. Firstly, we provide a proof that chained Bell inequalities can be used to robustly self-test maximally entangled pair of qubits and an arbitrary number of real measurements. As a side result we also present a protocol for randomness generation based on the maximal violation of a chained Bell inequality. Secondly, we provide new self-testing protocols for several classes of multipartite quantum states: Dicke states, graph states and all states of arbitrary finite dimension admitting the Schmidt decomposition. Finally, we extend self-testing to the semi-device-independent scenario and explore its properties.

In the second part of the thesis we move to the certification of several quantum resources and protocols. While the device-independent scenario offers the utmost security, it has a few undesirable properties. Firstly, it is very difficult to implement. In some cases, depending on the scenario, stronger assumptions about the functioning of the devices can be made. Secondly, the scenario relies on the observation of nonlocal measurement correlations, which makes some classes of entangled states useless for device-independent protocols. We address the first difficulty by presenting quantification of entanglement and randomness in quantum networks in the measurement-device-independent scenario, in which parties are assumed to have characterized preparation devices. In this scenario all entangled states can be detected. To address the second issue, we merge measurement-device-independent entanglement detection with self-testing and present the first protocol for a completely device-independent detection of all entangled states. The protocol involves placing an entangled state to be detected in a quantum network. Finally, we identify quantum state teleportation as a representative of one-sided measurement-device-independent protocols, which helps us to propose a new benchmark for certifying the non-classicality of teleportation. By using this new benchmark we show that all entangled states can lead to a teleportation experiment that cannot be simulated classically.

Resum

Les dues darreres dècades han significat un període molt fructífer per a la investigació bàsica en relació a la teoria quàntica de la informació. Avui en dia tenim un grau de comprensió raonable sobre l'efecte que les propietats quàntiques tenen de manera intrínseca sobre diverses tasques computacionals i criptogràfiques. Paral·lelament, també es produeixen avenços en les implementacions pràctiques: Varis dispositius que realitzen distribució quàntica de claus o generació quàntica de nombres aleatoris són ja una realitat i estan disponibles comercialment. Mentrestant, més i més recursos s'estan invertint en construir un dispositiu que pugui provar i explotar l'anomenada superioritat quàntica. En el context d'aquesta imminent segona revolució quàntica, la importància de construir noves eines de certificació, millorar les existents i entendre els seus límits és crucial. En el procés d'avaluar la no-classicalitat d'un dispositiu donat, és essencial poder estimar quines hipòtesis sobre el dispositiu no comprometen el procés de certificació. L'escenari independent del dispositiu (device-independent) no fa cap hipòtesi sobre el funcionament intern dels dispositius, tan sols pren com a punt de partida que la teoria quàntica és correcta. Aquest escenari ha guanyat molta atenció perquè aconsegueix certificar el caràcter quàntic de certs dispositius, fins i tot en el supòsit que adversaris potencials tenen a la seva disposició tot el poder que les lleis de la física permeten. El tema principal d'aquesta tesi és la certificació de diversos recursos quàntics de manera independent del dispositiu.

En la primera part de la tesi ens centrem en l'autoavaluació (self-testing), un dels protocols independents del dispositiu més senzills. El seu objectiu és recuperar els estats quàntics que s'usen, només a partir de les correlacions observades al mesurar. Té una importància fonamental en el paradigma independent del dispositiu ja que mostra quins estats quàntics deixen una 'empremta'. A la pràctica, significa un primer pas necessari per a protocols molt més complexes com ara la computació quàntica a cegues o la generació quàntica de claus aleatòries. En aquesta tesi presentem varis resultats referents a l'autoavaluació. Primerament, demostrem que les desigualtats de Bell encadenades poden ser usades per auto-avaluar parelles de qubits màximament entrellaçats de manera robusta, així com estats de Dicke, estats de grafs i estats de dimensió finita arbitrària que admetin la descomposició de Schmidt. Finalment, estenem l'autoavaluació a l'escenari semi-independent del dispositiu i n'explorem les seves propietats.

En la segona part de la tesi anem a la certificació de varis recursos quàntics i protocols. Mentre que l'escenari independent del dispositiu ofereix seguretat en grau màxim,

té algunes propietats que hom voldria evitar. Primerament, és difícil d'implementar: En alguns casos, depenent de la situació, es poden plantejar hipòtesis més fortes sobre el funcionament dels dispositius. En segon lloc, l'escenari es basa en l'observació de correlacions no locals, cosa que inutilitza certes classes d'estats entrellaçats per a protocols independents del dispositiu. Abordem el primer repte presentant una quantificació de l'entrellaçament i l'aleatorietat en xarxes quàntiques en l'escenari de mesurament independent del dispositiu, on se suposa que totes les parts tenen els seus aparells de preparació caracteritzats. En aquest cas, es poden detectar tots els estats entrellaçats. Quant al segon problema, combinem l'escenari de la mesurament independent del dispositiu amb l'autoavaluació i presentem el primer protocol per a una detecció de tots els estats entrellaçats de manera independent del dispositiu. El protocol implica la col·locació d'un estat entrellaçat per ser detectat en una xarxa quàntica. Finalment, identifiquem la teleportació d'estats quàntics com un representant dels protocols unilaterals de mesurament independent del dispositiu, el qual ens ajuda a proposar un nou punt de referència per certificar la no-classicalitat de la teleportació. Partint d'aquest punt de referència, demostrem que tots els estats entrellaçats indueixen un experiment de teleportació que no pot ser simulat de manera clàssica.

List of publications

1. *Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems*, J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, R. Augusiak, arXiv:1807.03332 (2018)

2. *Estimating entanglement in teleportation experiments*, I. Šupić, P. Skrzypczyk, D. Cavalcanti, arXiv:1804.10612 (2018)

3. *Experimental study of nonclassical teleportation beyond average fidelity*, G. Carvacho, F. Andreoli, L. Santodonato, M. Bentivegna, V. D'Ambrosio, P. Skrzypczyk, I. Šupić, D. Cavalcanti, F. Sciarrino, arXiv:1802.10056, (2018)

4. *Device-independent entanglement certification of all entangled states*, J. Bowles, I. Šupić, D. Cavalcanti, A. Acín, arXiv:1801.10444, (2018)

5. *Self-testing of Pauli observables for device-independent entanglement certification* J. Bowles, I. Šupić, D. Cavalcanti, A. Acín, arXiv:1801.10446, (2018)

6. *A simple approach to self-testing multipartite states*, I. Šupić, A. Coladangelo, R. Augusiak, A. Acín, arXiv: 1707.06534, (2017)

7. *Measurement-device-independent entanglement and randomness estimation in quantum networks*, I. Šupić, P. Skrzypczyk, D. Cavalcanti, PRA 95 (4), 042340, (2017)

8. *All Entangled States can Demonstrate Nonclassical Teleportation*, D. Cavalcanti, P. Skrzypczyk,I. Šupić, PRL 119 (11), 110501, (2017)

9. *Self-testing through EPR-steering*, I Šupić, M. J. Hoban, NJP 18 (7), 075006, (2016)

10. *Self-testing protocols based on the chained Bell inequalities* I Šupić, R. Augusiak, A. Salavrakos, A. Acín, NJP, 18 (3), 035013, (2016)

Contents

Acronyms list

CHSH - Clauser-Horne-Shimony-Holt
EPR - Einstein, Podolsky, Rosen
GHZ - Greenberger-Horne-Zeilinger
GME - genuinely multipartite entangled
GMN - genuinely multipartite nonlocal
LHS - local hidden state
LHV - local hidden variable
POVM - positive-operator valued measure
PPT - positive partial transpose
QKD - quantum key distribution
SDP - semidefinite programming
SOS - sum of squares
BQC - blind quantum computing
AST - robust assemblage-based one-sided self-testing
CST - robust correlation-based one-sided self-testing
DI - device-independnet
MDI - measurement-device-independent
MDIEW - measurement-device-independent entanglement witness
UPB - unextendable product bases
QKD - quantum key distribution
DIQKD - device-independent quantum key distribution
MDIQKD - measurement-device-independent quantum key distribution
NPA - Navascues-Pironio-Acin hierarchy

Chapter 1

Introduction and motivation

The groundbreaking significance of quantum mechanics and its status as one of the most successful theories are well established. The first half of the previous century was marked by the shift of the scientific paradigm based primarily on the mathematical and philosophical foundations of quantum theory but even more on its overwhelming success in explaining existing and predicting new phenomena. Some of the most successful consequences are the theories of atomic structure, chemical reactions, superconductivity, neutron stars, quantum electrodynamics, the structure of hadrons and the Standard model. Quantum theory has spanned its validity to all physical aspects of our world, except for gravity. While being strikingly successful as a fundamental scientific theory it also made a huge impact on the development of modern-day technologies. Discovery of transistors, lasers, superconductors, solar cells etc., termed as the first quantum revolution came as a result of the profound understanding of the structure of matter offered by quantum theory.

Another scientific trademark of the twentieth century are the pioneering works of Turing [Tur37] and Shannon [Sha48], which laid the foundations of the information theory and computer science. Only together with the emergence of these abstract theories could the discoveries related to the first quantum revolution lead to the rise of the Information age we live in. However, the contribution of quantum theory to information processing did not end there. A qualitatively different alliance between quantum and information theory led to the development of a new interdisciplinary field, quantum information theory. The central idea is that information processing protocols can be improved by harnessing authentically quantum behavior. At the core of the quantum advantages for information processing lie non-classical correlations stemming from quantum entanglement [HHHH09]. The results obtained in the last few decades in quantum information processing are heralds of a new age for quantum technologies, sometimes termed as the second quantum revolution. The main technological advancements related to this second quantum revolution are supposed to be quantum computers [Pre18] and various quantum communication systems with the emphasis on the cryptographic applications [BLMS00].

Such quantum devices can perform tasks which cannot be done, nor simulated efficiently, by any classical machine.

At the time when we anticipate a wide commercial use of quantum devices the problem of their certification becomes critically important. How can one ensure that some quantum device operates according to its specifications if it performs a task which cannot be simulated with the available technology? If the device produces a sequence of random numbers [AM16], how can one be sure that the sequence is genuinely random and not created by some pseudorandom number generator [Ruk+10]? Similarly, if a quantum computer is supposed to solve a problem which cannot be efficiently solved even with a superpowerful classical computer how can one certify the authenticity of the solution and the device? The importance of reliable certification techniques is furthermore dictated by the operating scenario of such devices, which must take into account potential adversarial activities. In view of this, the certification should be ideally performed with the minimal amount of assumptions on the inner functioning of devices. Such scenario exists and is called device-independent [Aci+07, CK11], since it drives conclusions solely from certain data correlations obtained from a process in which all devices are treated as black boxes. Quantum information protocols in device-independent scenario are formulated taking into account devices which are subject to arbitrary noise or even malicious adversarial activites. The direct characterisation of devices used in some quantum information protocol is many times a very complicated process, even more so if the protocol involves entangled states of many particles. Certification performed in a device-independent manner promises the unprecedented level of reliability, mostly because it bypasses the verification of a specific physical implementation of the corresponding protocol.

The main subject of this thesis is the *device-independent certification of quantum resources*. In the rest of this introductory section we will present several certification problems and outline the contributions derived in this thesis.

- **Device-independent certification of quantum states - self testing.**
  The basic constituents of almost every quantum information protocol are a source of an entangled quantum state and one or more measurement devices. Ensuring that the source functions according to its specifications in the device-independent setting is termed self-testing [MY04]. It is one of the crucial steps towards ensuring the security/validity of the protocol. Self-testing can be done on its own before continuing with the protocol, i.e. it can be a prerequisite for the protocol (as in the case of delegated quantum computing [RUV13]) or it can be hidden as an integral part of the protocol (as in the case of device-independent quantum key distribution or randomness generation [Aci+07]). On its own self-testing can be considered to be the most fundamental device-independent protocol and as such it drew a significant attention within the quantum information community in the last years

[BP15, Wu+14, PVN14, McK14, MYS14, YVBSN14, Kan16, Kan17, CGS17]. The aim is to have practically useful self-testing protocols for a wide range of pure entangled quantum states.

Our contributions:

- ⋆ We proved that the family of Bell inequalities named chained Bell inequalities [Pea70], maximally violated by the maximally entangled states and an arbitrary number of measurements is self-testing the state and measurements leading to the maximal violation [ŠASA16]. The presented self-testing protocol is robust. As a direct consequence, we proved that the maximal violation of any chained Bell inequality can be used for randomness certification.
- ⋆ We made another contribution in a, rather unexplored, self-testing of multipartite quantum states [ŠCAA17]. By extending the results from self-testing bipartite quantum states, we proved that a large class of multipartite qubit states can be self-tested. Among them are the multipartite qudit states admitting the Schmidt decomposition, which is the first self-test of some multipartite qudit state.

- **Semi-device-independent approach to self-testing.**
While offering the utmost security of quantum protocols, the device-independent scenario in some cases may be a surplusage. For example, in some cases one party, involved in the protocol, is building their own measurement device. In that case it makes sense to treat the measurement device as characterized and use it to perform quantum state tomography. Also, one or more parties involved in a protocol may have a trusted preparation device or be able to bound dimension of their system. Any additional trusted resource characterizes a different kind of semi-device-independent scenario. Since many times it is quite challenging to perform fully device-independent protocols, various semi-device-independent approaches gained a lot of attention and proved to be quite useful for some tasks. In this thesis we explored how self-testing behaves when full device-independence is dropped.

Our contributions:

- ⋆ First, we explored the properties of self-testing in the one-sided-device-independent scenario when one or more parties are able to perform tomography of their share of the state [ŠH16]. We defined two different approaches to self-testing in this scenario, assemblage-based and correlation-based. While obtaining a better tolerance to experimental errors we show that this improvement is only constant. Unlike some other tasks, the state certification does not benefit qualitatively from the one-sided-device-independent scenario compared to the fully device-independent.

    - ⋆ We defined self-testing in the measurement-device-independent scenario, where all parties have access to a characterized preparation device and can use quantum states as inputs for their measurement devices [DŠHA18]. This type of state certification is placed at the transition between full state tomography and device-independent self-testing. We are able to prove that every pure entangled quantum state can be certified in this way. Also, we define a numerical approach to measurement-device-independent state certification, based on the generalization of the Navascues-Pironio-Acín hierarchy [NPA07] to the scenario with quantum inputs.

- **Certifying quantum state teleportation.**
  Quantum state teleportation [Ben+93] is one of the linchpins of quantum information theory. It is the main building block of more advanced protocols such as cryptographic tasks [GRTZ02], quantum repeaters [BDCZ98], quantum computing [GC99, RB01] and many others. For its ubiquitous character in quantum information processing, it is of crucial importance to find the best way to certify its non-classicality and understand its relation to other fundamental concepts such as entanglement and nonlocality. Usually, the non-classicality of a teleportation protocol is witnessed by demonstrating an average teleportation fidelity larger than the one that can be achieved by any classical teleportation protocol.

  Our contributions:

    - ⋆ In [CSŠ17] we introduced a new benchmark to certify non-classicality of a teleportation protocol, taking into account all available data. The certification can be done by performing a semi-definite programming (SDP) optimization, whose dual form gives a teleportation witness. Using this benchmark we can show that every entangled state, including those which cannot reach a better average teleportation fidelity than separable states can produce teleportation data which cannot be simulated classically,
    - ⋆ Using the same benchmark we introduce several different quantifiers of quantum teleportation and relate them to the corresponding entanglement quantifiers.

- **Certifying entanglement and randomness in quantum networks.**
  The detection of entanglement in quantum networks consisting of many parties is one of the important steps towards building quantum communication and computation networks. In the emergence of such networks, it is beneficial to understand the simplest ways to detect and quantify entanglement in a network, using any available resource.

Our contributions:

- ⋆ We consider a scenario where the measurement devices used for this certification are uncharacterized. In this case, it is well known that by using quantum states as inputs for the measurement devices it is possible to detect any entangled state (a situation known as measurement device-independent entanglement witnessing [Bus12, BRLG13, RBGL13, CHW13, Hal16]). Here we go beyond entanglement detection and provide methods to estimate the amount of entanglement in a quantum network [ŠSC17]. We also consider the task of randomness certification and show that randomness can be certified in a variety of cases, including single-partite experiments or setups using only separable states.

- **Device-independence detection of entanglement.**
The device-independent paradigm is inherently related to the fact that a Bell inequality violation certifies the presence of entanglement. In turn, entanglement detection is one of the most fundamental device-independent tasks. The solution to this task in a device-independent way does not come immediately, because not every entangled state violates a Bell inequality [Wer89]. Different variants of the standard Bell scenario were suggested, but none of them proved to be convenient for obtaining nonlocality from every entangled state.

Our contributions:

- ⋆ We construct the first protocol to certify the entanglement of all entangled quantum states in a fully device-independent manner [BŠCA18]. Entanglement is certified from a correlation inequality based on the appropriate entanglement witness. The proposed scenario differs from the Bell test in adding auxiliary parties, i.e. placing the state of interest in a quantum network. The protocol borrows ideas from self-testing and measurement-device-independent entanglement certification. As a by-product, we present a self-test of the tensor products of Pauli measurements on *n* copies of the maximally entangled pairs of qubits [BŠCA18a].

We expect that the work presented in this thesis will be helpful for constructing certification tools for complex quantum devices and bridge the gap between rich theoretical insights and emerging practical implementations.

Chapter 2

Preliminaries

In this chapter, we review some of the basic concepts that we use in the rest of this thesis. The central concepts of this thesis, those of entanglement and nonlocality, are discussed in Sections 2.1 and 2.2, respectively. Einstein-Podolsky-Rosen (EPR) steering, a concept halfway between entanglement and nonlocality, is the subject of Section 2.4. Section 2.3 briefly recapitulates the main ideas behind the device-independent approach to quantum information theory. Self-testing, one of the most basic device-independent protocols, is the subject of Section 2.5. The randomness that emerges from nonlocal correlations is described in Section 2.6. Finally, semidefinite programming, a widely-used technique in this thesis, is reviewed in Section 2.7.

2.1 Quantum entanglement

Quantum entanglement is one of the main distinctive features of quantum theory. It was first described in the works of Einstein, Podolsky and Rosen [EPR35] and Schrödinger [Sch35], who coined the term ’entanglement’. The existence of entangled states is the consequence of the superposition principle and the structure of the state space of multipartite systems. Namely, a pure state of a single particle is a unit-norm vector in a Hilbert space, while a pure state of two particles is a vector in the tensor product of two Hilbert spaces $\mathscr{H}^{\mathrm{A}} \otimes \mathscr{H}^{\mathrm{B}}$. A pure state of two particles $|\psi\rangle^{\mathrm{AB}}$ is called a product state if it can be written as the tensor product of states of each particle,

$$|\psi\rangle^{\mathrm{AB}} = |\phi\rangle^{\mathrm{A}} \otimes |\xi\rangle^{\mathrm{B}}.$$

States that are not product are entangled. One example of entangled states is the so-called singlet state

$$|\Psi^{-}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

A mixed state is a statistical ensemble of pure states. It is described by a density matrix, defined in the following way

$$\rho^{\mathrm{AB}} = \sum_j v_j \left|\psi_j\right\rangle \left\langle\psi_j\right|,$$

where $\left|\psi_j\right\rangle$ are pure states and v_j positive numbers summing up to one. A mixed state is called separable if it can be written as a convex combination of product states:

$$\rho^{\mathrm{AB}} = \sum_j p_j \rho_j^{\mathrm{A}} \otimes \rho_j^{\mathrm{B}}.$$

If it is not the case, the mixed state is said to be entangled.

The concept of entanglement straightforwardly generalizes to multipartite systems, but states of more than two particles exhibit a richer entanglement structure. For example, a state of three particles ρ^{ABC} is fully separable if it can be written as

$$\rho^{\mathrm{ABC}} = \sum_j p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|^{\mathrm{A}} \otimes \left|\phi_j\right\rangle \left\langle\phi_j\right|^{\mathrm{B}} \otimes \left|\xi_j\right\rangle \left\langle\xi_j\right|^{\mathrm{C}}. \tag{2.1}$$

If ρ^{ABC} cannot be written in this form it is entangled. A state ρ_a^{ABC} that cannot be written in the form (2.1) but admits the following decomposition

$$\rho_a^{\mathrm{ABC}} = \sum_j p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|^{\mathrm{A}} \otimes \left|\phi_j\right\rangle \left\langle\phi_j\right|^{\mathrm{BC}}.$$

is said to be separable across the bipartition A|BC. Analogously, it is possible to define states which are separable across different bipartitions and denote them by ρ_b^{ABC} (separable across the bipartition AC|B) and ρ_c^{ACB} (separable across bipartition AB|C). Finally, a state is said to be biseparable if it can be written as a convex combination of states that are separable across some bipartition:

$$\rho^{\mathrm{ABC}} = p_a \rho_a^{\mathrm{ABC}} + p_b \rho_b^{\mathrm{ACB}} + p_c \rho_c^{\mathrm{ABC}}, \qquad p_a + p_b + p_c = 1.$$

A state ρ^{ABC} is said to be genuinely multipartite entangled (GME) if it is not biseparable.

For a long time entangled states were the subject of research strictly related to the foundations of quantum theory. An inflation of the works related to the theory of quantum entanglement came with the development of quantum information theory. In the last decades entanglement has been scrutinized no only as a curious aspect of quantum theory, but also as a pivotal resource for quantum information processing. Quantum cryptography [BLMS00], quantum computing [NC00], quantum randomness generation [AM16] and recently quantum machine learning [Bia+17] all use entanglement as one of their primary resources. The most famous entangled states in quantum information theory are maximally entangled pairs of qubits, or 'Bell states':

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

These states are used in pioneering quantum information protocols such as quantum state teleportation [Ben+93], superdense coding [BW92], quantum key distribution [Eke91]. Since the four Bell states can be transformed into each other by applying a local unitary transformation, they all represent the same resource, and the state $|\Phi^+\rangle$ is usually taken to be the representative. Due to their practical importance, the question of how to extract Bell pairs from some amount of arbitrary mixed entangled states gained a lot of attention. A protocol that starts from n copies of some entangled state ρ, applies some local operations and classical communication (LOCC) and ends up with m ($m \leq n$) copies of $|\Phi^+\rangle$ is called distillation of entanglement [BBPS96, Ben+96]. States that are entangled but useless in a distillation protocol are called bound entangled states [HHH99].

2.1.1 Detection of entanglement

The central problem of entanglement theory is to find simple and efficient entanglement detection criteria. There is not much hope of finding a universal and efficient criterion, since determining if an arbitrary state is entangled or not belongs to the class of NP-hard problems [Gur04]. However, for some instances of states, the problem can be easily solved. For example, for every pure bipartite state $|\psi\rangle^{\mathrm{AB}} \in \mathbb{C}^{d_\mathrm{A}} \otimes \mathbb{C}^{d_\mathrm{B}}$, there exist two local bases called 'Schmidt bases', in which the state has the Schmidt form

$$|\psi\rangle^{\mathrm{AB}} = \sum_{j=1}^{s} \lambda_j \, |j\rangle^{\mathrm{A}} \, |j\rangle^{\mathrm{B}}. \tag{2.2}$$

The number $s \leq \min(d_\mathrm{A}, d_\mathrm{B})$ is called the Schmidt rank, and it is bigger than one if and only if $|\psi\rangle^{\mathrm{AB}}$ is entangled.

A necessary condition for a mixed state to be entangled was formulated by Peres [Per96], and it consists in checking positivity of the partial transpose of a density matrix. Separable states have positive partial transpose:

$$\left(\rho^{\mathrm{AB}}\right)^{T_A} = \sum_i p_i \left(\rho_i^{\mathrm{A}}\right)^T \otimes \rho_i^{\mathrm{B}} \geq 0,$$

because transposition is a positive map. However, positivity of the partial transpose is not a sufficient condition, except for the states whose product of local dimensions is not

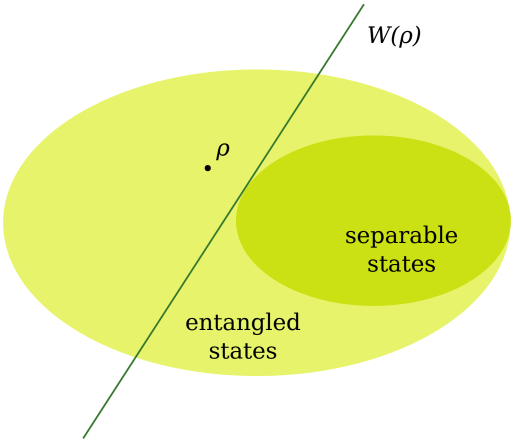

Figure 2.1: A representation of the sets of separable and all quantum states. The set of separable states is a convex subset of the set of all quantum states. By virtue of the Hahn-Banach theorem, for every entangled state ρ there exists an entanglement witness such that $\mathrm{tr}(W\rho_{sep}) > 0$ for every separable state ρ_{sep}, but $\mathrm{tr}(W\rho) < 0$.

bigger than six [HHH96]. This condition is usually named PPT criterion and states with positive partial transpose are called PPT states.

Since the set of separable states is convex, its characterisation can be facilitated by using the Hahn-Banach separation theorem [Kre89].

Theorem 1. *If S and E are disjoint closed convex subsets of a Banach space X, and S is compact, then there exists a continuous linear functional f on X such that*

$$\sup_{x\in S} f(x) \leq \inf_{y\in E} f(y).$$

As a consequence of this theorem, for every entangled state, there is a linear functional separating it from the set of separable states. By the Riesz representation theorem [Kre89], the space of linear functional is isomorphic to the set of bounded linear operators. We can thus formulate the following corollary:

Corollary 1.1. *[Ter00] For every entangled state ρ, there exists a Hermitian operator W such that $\mathrm{tr}[W\rho] < 0$ and $\mathrm{tr}[W\sigma] > 0$ for all separable states σ. The operator W is called entanglement witness and it witnesses the entanglement of the state ρ.*

Equivalently, the observable W is an entanglement witness if it has at least one negative eigenvalue, but gives positive value when evaluated on any separable state. Entanglement witnesses are very important because they can be physically implemented, henceforth they are the most common way to detect or certify entanglement in an experiment. However, there is no a universal method for constructing entanglement witnesses, since Corollary 1.1 only states that there exists an entanglement witness for every entangled state, but says nothing about a way to find its form. A lot of effort has been invested in constructing entanglement witnesses and there is extensive literature on the topic (see [GT09] and references therein), but it is beyond the scope of this technical introduction to go into further details.

In an experiment, entanglement can also be detected by observing non-local measurement correlations. This approach will be detailed in Section 2.2.

2.1.2 Quantification of entanglement

Entangled states can be seen as a resource for various quantum information processing tasks. The benchmark for success in those tasks is often the best performance of a classical, i.e. a separable state. Different entangled states behave differently and thus the problem of entanglement quantification naturally emerges. For that purpose various entanglement measures have been developed. Before discussing in more details those that are relevant in the later chapters of this thesis, let us recall the necessary properties of a generic entanglement measure ε:

- it should be equal to zero for all separable states;
- it should be invariant under local unitary state transformations and non-increasing under local operations and classical communications, i.e. LOCC state transformations ;

The most famous entanglement measures are concurrence [HW97], entanglement cost [BDSW96, HHT01], entanglement of distillation [BDSW96], entanglement of formation [BDSW96], squashed entanglement [CW03] and two that we will describe in more details, entanglement negativity [VW02] and entanglement robustness [VT99].

The *entanglement negativity* is derived from the PPT criterion and quantifies how much a state violates it. Consequently it is equal to zero for all PPT entangled states. Formally, it is defined as

$$\mathscr{N}(\rho) = \frac{\|\rho^{T_{\mathrm{B}}}\|_1 - 1}{2}$$

This entanglement measure is widely used because it is easy to grasp, easy to compute and convex. Negativity also puts a bound on distillable entanglement and teleportation capacity [VW02]. A related measure is logarithmic negativity defined as $\log_s \|\rho^{T_{\mathrm{B}}}\|_1$ [Ple05]. Unlike negativity, it is additive, but not convex.

The *entanglement robustness* is one of the measures with a simple operational meaning. It is defined as the smallest amount of noise one can add to the state before it becomes separable and it is calculated as the solution to the following optimization problem

$$\begin{aligned} \mathscr{R}_{\Sigma}(\rho) = \max\nolimits_{\sigma} \quad & s \\ \text{s.t.} \quad & \frac{\rho + s\sigma}{1+s} \\ & \sigma \in \Sigma. \end{aligned}$$

Robustness is originally defined with Σ being the set of separable states [VT99]. If Σ is the set of all quantum states it defines the generalized entanglement robustness [Ste03, HN03]. Random robustness is obtained when $\sigma = \mathbb{1}/(d_{\mathrm{A}} d_{\mathrm{B}})$ (where d_{A} and d_{B} are the dimensions of the subsystems of the state ρ) [VT99] and no optimization over the space of states is needed.

2.2 Nonlocal correlations

The concept of entanglement was introduced as a challenge for the completeness of quantum theory. The famous EPR paper [EPR35] presented an entangled state that leads to measurement results which either violate the Heisenberg uncertainty principle or imply superluminal transmission of information. To resolve the paradox, Einstein, Podolsky and Rosen suggested the existence of some kind of hidden variables which would assign measurement outcomes to quantum mechanical observables and in that way complete the theory. Three decades after the EPR paper was published, John Stewart Bell examined the properties of theories admitting local hidden variable models [Bell64]. He started from an abstract theory satisfying two conditions suggested in the EPR paper:

- *reality* i.e. the properties of a system exist prior to and independent of a measurement process and they are only revealed by measurements. Instead of reality, some authors use words ’objectivity’ or ’determinism’.

- *locality*, i.e. measurements performed on some system cannot instantaneously affect measurements on some other, spatially distant, system, no matter what is the state of the two systems.

The main result of the paper was the famous Bell’s theorem which showed that there are bounds on the measurement correlations which can be achieved by any theory satisfying the two above given properties, i.e. for all theories admitting the existence of local hidden variables. These bounds are known as *Bell inequalities*. Importantly, Bell showed that quantum theory admits violations of Bell inequalities. Concisely Bell’s theorem can be stated as

Theorem 2. *[Bell64] No local hidden variable theory can reproduce the measurement correlations admissible by quantum theory.*

Bell's conclusions were confirmed by various experimental corroborations [FC72, ADR81, TBZG98], particularly by three loophole-free Bell experiments (i.e. free from uncontrollable experimental deficiencies which could invalidate the conclusiveness of the experiment) [Hen+15, Giu+15, Sha+15].

The scenario of a Bell experiment, or a Bell test, involves two (or more) spatially separated parties, usually named Alice and Bob, who perform measurements on their shared state and provide measurement outcomes. The different measurements that can be performed are denoted by $x \in \{0,\dots,n_\mathrm{A}-1\}$ for Alice and $y \in \{0,\dots,n_\mathrm{B}-1\}$ for Bob. Alice's measurement outcomes are denoted with $a \in \{0,\dots,m_\mathrm{A}-1\}$, and Bob's with $b \in \{0,\dots,m_\mathrm{B}-1\}$. The final result of a Bell test is the set of probabilities, called *behaviour*:

$$\mathbf{P} = \{p(a,b|x,y)\},$$

which are used to evaluate the Bell expression

$$\mathscr{I} = \sum_{a,b,x,y} b_{a,b,x,y} p(a,b|x,y).$$

This is then compared with the benchmark given by the Bell inequality $\mathscr{I} \leq \beta_{LHV}$. The benchmark β_{LHV} is called the classical bound of the Bell inequality. For qualifying a Bell experiment, the following three statements are equivalent [Fine82]:

1. Behaviour $\mathbf{P}$ violates some Bell inequality.

2. There is no local hidden variable model reproducing behaviour $\mathbf{P}$.

3. Probabilities $p(a,b|x,y) \in \mathbf{P}$ cannot be decomposed as the product of local terms

$$p(a,b|x,y) = \int p_\lambda p(a|x,\lambda) p(b|y,\lambda) d\lambda. \tag{2.3}$$

Due to the inexistence of the decomposition 2.3, behaviours violating some Bell inequality are called *nonlocal*.
Quantum violations of Bell inequalities. In principle, it is possible for Alice and Bob to violate Bell inequalities by performing measurements $\{M_{a|x}\}$ and $\{M_{b|y}\}$, respectively, on their shared entangled state ρ^{AB}. The probability to obtain the pair of outcomes (a,b) when the pair of inputs is (x,y) is given by the Born rule

$$p(a,b|x,y) = \mathrm{tr}[(M^{\mathrm{A}}_{a|x} \otimes M^{\mathrm{B}}_{b|y})\rho^{\mathrm{AB}}].$$

Let us revise the LHV bound and quantum violation for the simplest bipartite inequality, the Clauser-Horne-Shimony-Holt (CHSH) inequality, native to the scenario $n_\mathrm{A} = n_\mathrm{B} = m_\mathrm{A} = m_\mathrm{B} = 2$. It is given by the following expression

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle, \tag{2.4}$$

where correlator $\langle A_j B_k \rangle$ is calculated according to

$$\langle A_j B_k \rangle = \sum_{a,b} (-1)^{a+b} p(a,b|j,k).$$

Henceforth, every correlator must have some value between -1 and 1. To infer the maximal value of the expression (2.4) for LHV theories let us rewrite it as follows:

$$\langle A_0(B_0 + B_1) \rangle + \langle A_1(B_0 - B_1) \rangle.$$

To maximize this expression one can choose $\langle A_0 \rangle = \langle A_1 \rangle = 1$, i.e. measuring observables A_0 and A_1 always produces the outcome $+1$. Furthermore, the maximal value for $\langle B_0 + B_1 \rangle$ is 2, but in that case $\langle B_0 - B_1 \rangle = 0$, and the other way around. This is exactly the optimal strategy and thus the CHSH inequality is

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2, \tag{2.5}$$

By utilizing quantum resources Alice and Bob can violate this inequality. If they share Bell state $|\Phi^+\rangle$ and measure observables

$$\begin{aligned} A_0 &= \sigma_Z, & A_1 &= \sigma_X, \\ B_0 &= \frac{\sigma_Z + \sigma_X}{\sqrt{2}} & B_1 &= \frac{\sigma_Z - \sigma_X}{\sqrt{2}} \end{aligned}$$

the correlators have the form

$$\langle A_j B_k \rangle = \mathrm{tr}[(A_j \otimes B_k) |\Phi^+\rangle \langle \Phi^+|].$$

The violation that Alice and Bob can achieve in this way is

$$\mathrm{tr}\left[(A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1) |\Phi^+\rangle \langle \Phi^+|\right] = 2\sqrt{2},$$

which is the maximal violation of the CHSH inequality achievable in quantum theory [Tsi80].

2.2.1 Resources for nonlocality

The nonlocality of a behaviour **P** stems from non-classicality of both quantum state and measurements. As we have seen, nonlocal correlations are produced by entangled states. Apart from this, two or more of the measurements that each party performs have to be incompatible. In this section we discuss in more details relations between nonlocality on one side and entanglement and incompatibility on the other.

Entanglement and nonlocality. Entanglement is a necessary condition for nonlocality, since separable states cannot produce nonlocal probability distributions. Indeed, a separable state $\rho^{\mathrm{AB}} = \sum_\lambda p_\lambda \rho_\lambda^{\mathrm{A}} \otimes \rho_\lambda^{\mathrm{B}}$ produces probabilities which are the convex sums of products of local probabilites:

$$\begin{aligned} p(a,b|x,y) &= \mathrm{tr}[(M_{a|x}^{\mathrm{A}} \otimes M_{b|y}^{\mathrm{B}})\rho^{\mathrm{AB}}] \\ &= \sum_\lambda p_\lambda \mathrm{tr}[(M_{a|x}^{\mathrm{A}}\rho_\lambda^{\mathrm{A}}) \otimes (M_{b|y}^{\mathrm{B}}\rho_\lambda^{\mathrm{B}})] \\ &= \sum_\lambda p_\lambda p(a|x,\lambda)p(b|y,\lambda). \end{aligned}$$

For pure states entanglement is also a sufficient condition for nonlocality [Gis91]. However, there are mixed entangled states which cannot violate any Bell inequality, i.e. they are local [Wer89, Bar02]. To prove that an entangled state is local one needs to explicitly construct an LHV model for the probabilities obtained by applying any possible set of measurements. This is in principle a very difficult task, and describing methods used to achieve it goes far beyond the scope of this introductory chapter.

Beyond the bipartite scenario, similarly to multipartite entanglement, there are different ways in which some multipartite behaviour can be nonlocal. The strongest type of multipartite nonlocality is genuine multipartite nonlocality. In the tripartite scenario, the conditional probability distributios $p(a,b,c|x,y,z)$ are genuinely multipartite nonlocal (GMN) if they cannot be written in the following way

$$\begin{aligned} &\int d\lambda p_\lambda p(a|x,\lambda)p(b,c|y,z,\lambda)+ \\ &\qquad\qquad + \int d\mu p_\mu p(b|y,\mu)p(a,c|x,z,\mu)+ \\ &\qquad\qquad\qquad\qquad + \int d\nu p_\nu p(c|z,\nu)p(a,b|x,y,\nu). \end{aligned}$$

Contrarily, probability distributions allowing the above given factorization are called bilocal. Relation between genuine multipartite entanglement and genuine multipartite nonlocality for pure states is yet unresolved, while for mixed states these two concepts are inequivalent, i.e. there are GME states which are not GMN [ADTA15].

Incompatibility and nonlocality. Another nonclassical resource necessary for quantum nonlocality is measurement incompatibility. This is an purely quantum effect, since in classical physics all measurements are compatible, i.e. jointly-measurable. For projective measurements, incompatibility is equivalent to commutativity, but for general non-projective measurements, defined by positive-operator valued measures (POVMs) these two concepts are different. Two POVMs $\{M_a\}$ and $\{N_b\}$ are compatible if there exists a mother-POVM $\{R_{a,b}\}$ such that

$$\begin{aligned} \sum_{a,b} R_{a,b} = \mathbb{1}, \qquad & R_{a,b} \geq 0, \quad \forall a,b \\ \sum_{a} R_{a,b} = N_b, \qquad & \sum_{b} R_{a,b} = M_a. \end{aligned} \tag{2.6}$$

To show that measuring compatible observables leads to local behaviours let us first show the existence of a valid probability distribution $p(a_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1)$ such that

$$\begin{aligned} p(a_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1) &\geq 0, \quad \forall a_0,a_1,b_0,b_1,x_0,x_1,y_0,y_1; \\ \sum_{a_0} p(a_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1) &= p(a_1,b_0,b_1|x_1,y_0,y_1), \quad \forall a_1,b_0,b_1,x_0,x_1,y_0,y_1; \\ \sum_{a_1} p(a_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1) &= p(a_0,b_0,b_1|x_0,y_0,y_1), \quad \forall a_0,b_0,b_1,x_0,x_1,y_0,y_1; \\ \sum_{b_0} p(a_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1) &= p(a_0,a_1,b_1|x_0,x_1,y_1), \quad \forall a_0,a_1,b_1,x_0,x_1,y_0,y_1; \\ \sum_{b_1} p(a_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1) &= p(a_0,a_1,b_0|x_0,x_1,y_0), \quad \forall a_0,a_1,b_0,x_0,x_1,y_0,y_1. \end{aligned} \tag{2.7}$$

Probabilities $p(a_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1)$, satisfying (2.7), give a LHV model recovering $p(a,b|x,y)$ [Fine82]. To see this, note that $p(a_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1)$ can be treated as p_λ from (2.3). In this case the hidden variable λ is discrete and characterized by four indices $(\lambda_{a_0},\lambda_{a_1},\lambda_{b_0},\lambda_{b_1})$ which turns the integral from (2.3) into a sum. To obtain the observed correlation probabilities and marginals we use $p(a_j|x_k,\lambda) = \delta_{a_j,\lambda_{a_k}}$ and $p(b'_j|y'_k,\lambda) = \delta_{b'_j,\lambda_{b'_k}}$. We get

$$\begin{aligned} p(a_0,b_0|x_0,y_0) = \sum_{a_1,b_1} \Big(& 1\cdot 1\cdot p(a_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1) + 1\cdot 0\cdot p(a_0,\bar{a}_1,b_0,b_1|x_0,x_1,y_0,y_1) \\ & + 0\cdot 1\cdot p(\bar{a}_0,a_1,b_0,b_1|x_0,x_1,y_0,y_1) + 0\cdot 0\cdot p(\bar{a}_0,\bar{a}_1,b_0,b_1|x_0,x_1,y_0,y_1) \Big); \end{aligned}$$

and similarly for all the other correlation probabilities and marginals. Now, observe that if Alice or Bob measure compatible observables, they could measure the mother-observable instead and thus obtain the probability distribution satisfying Eq. (2.7). Let us assume that Alice, instead of measuring two compatible observables $M_{a_0|x_0}$ and $M_{a_1|x_1}$, measures the mother-observable $\tilde{M}_{a_0,a_1}$ satisfying conditions equivalent to (2.6): $\sum_{a_0} \tilde{M}_{a_0,a_1} = M_{a_1|x_1}$ and $\sum_{a_1} \tilde{M}_{a_0,a_1} = M_{a_0|x_0}$. This leads to the existence of probabilities $p(a_0,a_1,b|x_0,x_1,y)$ such that

$$\sum_{a_0} p(a_0,a_1,b|x_0,x_1,y) = p(a_1,b|x_1,y), \quad \sum_{a_1} p(a_0,a_1,b|x_0,x_1,y) = p(a_0,b|x_0,y), \quad \forall b,y$$

Now the set of probabilities $p(a_0,a_1,b|x_0,x_1,y)$ for different values of a_0,a_1,b,y plays the role of p_λ and can be used to construct an LHV model in a similar way as described in the text above.

A nonlocal behaviour implies that both Alice and Bob used incompatible measurements, henceforth measurement incompatibility is a necessary condition for nonlocality. However, it is not a sufficient condition for nonlocality, since there exist incompatible observables which cannot be used for the violation of Bell inequalities [BV17, HQB17].

2.2.2 The set of quantum correlations

A quantum behaviour is the set of conditional probabilities

$$\mathbf{P}_{\mathscr{Q}} = \{p(a,b|x,y)\},$$

such that there is a quantum state $\rho^{\mathrm{AB}} \in \mathbb{B}(\mathscr{H}^{\mathrm{A}} \otimes \mathscr{H}^{\mathrm{B}})$ and POVMs $\{M_{a|x}\}$ and $\{M_{b|y}\}$ satisfying

$$p(a,b|x,y) = \mathrm{tr}[(M_{a|x} \otimes M_{b|y})\rho^{\mathrm{AB}}], \qquad \forall a,b,x,y. \tag{2.8}$$

Since we are not imposing any bound on the dimensions of the Hilbert spaces $\mathscr{H}^{\mathrm{A}}$ and $\mathscr{H}^{\mathrm{B}}$, we can always purify the mixed state ρ^{AB} into a pure state in a space of a larger dimension and use Naimark extensions of POVMs $\{M_{a|x}\}$ and $\{M_{b|y}\}$ to express them as a projective measurements. Thus, we can reduce the problem to finding a pure state $|\psi\rangle$ and projective measurements $\{\Pi_{a|x}\}$ and $\{\Pi_{b|y}\}$ such that

$$p(a,b|x,y) = \langle\psi|\, \Pi_{a|x} \otimes \Pi_{b|y} \,|\psi\rangle\,, \qquad \forall a,b,x,y. \tag{2.9}$$

By definition, all probabilities $p(a,b|x,y)$ are positive and normalized

$$\sum_{a,b} p(a,b|x,y) = 1.$$

One of the big open questions of quantum foundations is the characterisation of the set of quantum correlations (or quantum behaviours) $\mathscr{Q}$. By characterising $\mathscr{Q}$ we understand finding a criterion which would suffice to infer if a given behaviour belongs to $\mathscr{Q}$ or not. The solution to this problem could have a significant impact on quantum information theory. For every quantum information processing task it is of essential importance to estimate the best possible performance of quantum strategies. The more accurate characterisation of the set of quantum correlations (quantum set in the further text), the better is our understanding of the advantages and limits of quantum resources in different tasks.

The best available approximation of the quantum set is given by the Navascues, Pironio, Acín (NPA) hierarchy [NPA07]. It represents a hierarchy of supraquantum sets, corresponding to the successive levels of the hierarcchy, each of which provides a tighter approximation to the quantum set. In the limit of infinite level the hierarchy converges to the quantum set. In principle it can converge at some finite level but there is no general rule telling if such convergence occurs or not. To each level of the hierarchy corresponds a supraquantum set which can be easily characterized with semidefinite programming techniques. The main idea of the method is the existence of a map between quantum behaviours and positive-semidefinite matrices. Let the set of operators $M \equiv \{M_i\} = \{M_{a|x} \otimes \mathbb{1}, \mathbb{1} \otimes N_{b|y}\}$ satisfy constraints of quantum measurement operators. The labelled set

$$O^{(n)} \equiv \{O_i\} = \{M_i\}_i \cup \{M_i M_j\}_{i,j} \cup \dots \cup \left\{ \prod_{i=1}^{n} M_i \right\}, \tag{2.10}$$

can be used to construct a n-th level moment matrix $\Gamma^{(n)}$ according to the following rule

$$\Gamma^{(n)}_{i,j} = \langle \psi | O_i^\dagger O_j | \psi \rangle, \tag{2.11}$$

where $|\psi\rangle$ is a quantum state. Some entries of the moment matrix are the observable probabilities $\langle \psi | M_{a|x} \otimes N_{b|y} | \psi \rangle$, while the others are unknown and, moreover, unobservable quantities. The existence of a positive semidefinite matrix built according to the rules (2.11) with certain entries being elements of a behaviour $\mathbf{P}$ represents a certificate for that behaviour. In other words, the existence of a positive semidefinite matrix $\Gamma^{(n)}$ built from the elements of a behaviour $\mathbf{P}$, tells that the behaviour belongs to a supraquantum set $\mathscr{Q}_n$. The succession of the supraquantum sets $\{\mathscr{Q}_n\}_n$ satisfies the relation $\mathscr{Q}_{n+1} \subset \mathscr{Q}_n$, with $\lim_{n\to\infty} \mathscr{Q}_n = \mathscr{Q}$. If a certificate does not exist for some n, the behaviour $\mathbf{P}$ does not belong to the quantum set. NPA hierarchy is commonly used for finding the upper bound to the maximal quantum violation of some Bell inequality.

Local set. The elements of the behaviours belonging to the local set allow for the form given in (2.3):

$$\mathbf{P}_L \in \mathscr{L} \quad \Leftrightarrow \quad p(a,b|x,y) = \int d\lambda\, p_\lambda\, p(a|x,\lambda) p(b|y,\lambda), \quad \forall a,b,x,y.$$

The hidden variable λ is distributed according to the probability distribution p_λ, and $p(a|x,\lambda)$ and $p(b|y,\lambda)$ are local response functions depending on the given input and the value of the hidden variable. Every element from the local set can be written in the form (2.9), impling that $\mathscr{L}$ is a subset of the quantum set $\mathscr{Q}$. Since $\mathscr{L}$ is closed and convex and strictly contained in $\mathscr{Q}$, the Hahn-Banach separation theorem (1) applies. For every quantum behaviour **P'** $= \{p'(a,b|x,y)\}$ not belonging to $\mathscr{L}$ there is a hyperplane separating it from $\mathscr{L}$. This hyperplane represents a Bell inequality violated by **P'**:

$$\begin{aligned} \mathscr{I} = \mathbf{b} \cdot \mathbf{P}_L = \sum_{a,x,b,y} b_{a,x,b,y} p(a,b|x,y) &\leq \beta_{LHV} \qquad \forall \mathbf{P}_L \in \mathscr{L}, \\ \mathbf{b} \cdot \mathbf{P'} &> \beta_{LHV}. \end{aligned}$$

One such hyperplane in the scenario of two parties measuring two dichotomic observables each, corresponds to the aforementioned CHSH inequality. The local set is identified to be the convex hull of a finite number of deterministic local hidden variable models [BCPSW14]. Thus, the local set $\mathscr{L}$ is actually a polytope, usually called the local polytope and its vertices are the deterministic local hidden variable models. Equivalently, the local polytope can be characterized by a finite number of Bell inequalities, called facets or tight Bell inequalities.

No-signalling set. The set of no-signalling behaviours $\mathscr{N}\mathscr{S}$ is the largest set of correlations which can be physically observed, since it is bounded only by the no-signalling principle. The elements of a behaviour $\mathbf{P} \in \mathscr{N}\mathscr{S}$ are such that

$$\begin{aligned} \sum_a p(a,b|x,y) &= \sum_a p(a,b|x,y'), \qquad \forall b,x,y,y' \\ \sum_b p(a,b|x,y) &= \sum_b p(a,b|x',y), \qquad \forall a,x,x',y. \end{aligned} \tag{2.12}$$

These constraints rule-out non-physical behaviours in which Alice and Bob can signal to each other instantaneously by simply choosing different inputs. Every element of the quantum set satisfies constraints 2.12, implying $\mathscr{Q} \subset \mathscr{N}\mathscr{S}$. The no-signalling set is also a polytope. Furthermore, the Hahn-Banach theorem applies for all no-signalling behaviours outside of the quantum set. Hyperplanes separating such points from the quantum set are called Tsirelson inequalities [Tsi93]. However, since the quantum set is not a polytope, one would need an infinite number of Tsirelson inequalities to characterize the quantum set.

2.2.3 Examples of Bell inequalities

In this section we will define a few important (classes of) Bell inequalities, which will be relevant in the later stages of this thesis.

Tilted CHSH inequality. The tilted CHSH inequality, introduced in [AMP12], is another important Bell inequality in the scenario where two parties measure two dichotomic observables each. It differs from the CHSH inequality by taking into account a marginal term of one of the measured observables. Let us denote by A_j and B_j ($j = 0, 1$) the observables of Alice and Bob, respectively, and denote their outcomes with ± 1. The tilted CHSH inequality reads

$$\mathscr{I}_{tilt} = \alpha\langle A_0\rangle + \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leq \alpha + 2, \tag{2.13}$$

where $0 \leq \alpha < 2$. The quantum bound for this inequality is $\beta_Q = \sqrt{8+2\alpha^2}$ and it is

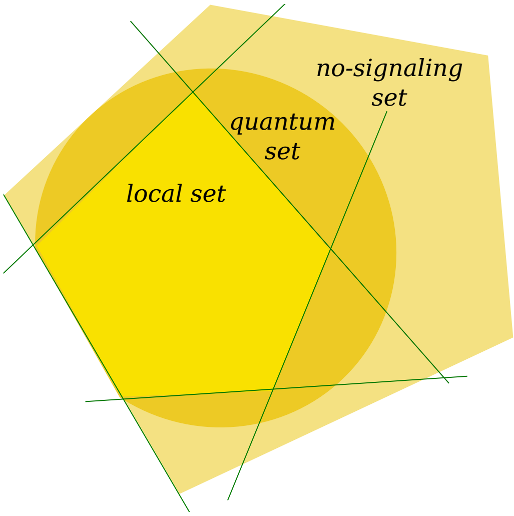

Figure 2.2: A possible configuration of different correlation sets. We see that the local set can be characterized by stating five facet Bell inequalities. Vertices of the local set are local deterministic strategies.

achieved by using the following strategy

$$\begin{aligned}
&|\psi_\theta\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle\,, \quad \tan 2\theta = \sqrt{\frac{2}{\alpha^2} - \frac{1}{2}}\\
&A_0 = \sigma_Z, \quad A_1 = \sigma_X,\\
&B_0 = \cos\mu\,\sigma_Z + \sin\mu\,\sigma_X, \quad B_1 = \cos\mu\,\sigma_Z - \sin\mu\,\sigma_X, \quad \tan\mu = \sin 2\theta.
\end{aligned}$$

For $\alpha = 0$ the tilted CHSH inequality reduces to the standard CHSH inequality.

Chained Bell inequalities. The chained Bell inequalities were introduced in Refs. [Pea70, BC90] to generalize the CHSH inequality to a larger number of measurements per party, while keeping the number of outcomes to two. Let us denote by A_i and B_i ($i = 1, \ldots, n$) the observables of Alice and Bob, respectively, and assume that they all have outcomes ±1. Then, the chained Bell inequality for n inputs reads

$$\mathscr{I}^n_{ch} = \sum_{i=1}^{n} \left(\langle A_i B_i\rangle + \langle A_{i+1} B_i\rangle\right) \leq 2n - 2 \tag{2.14}$$

where we denote $A_{n+1} \equiv -A_1$. Notice that for $n = 2$ the above formula reproduces the CHSH Bell inequality. It has been shown in [Weh06] that the maximal quantum violation of a chained Bell inequality (2.14) is

$$\beta_Q = 2n\cos\frac{\pi}{2n},$$

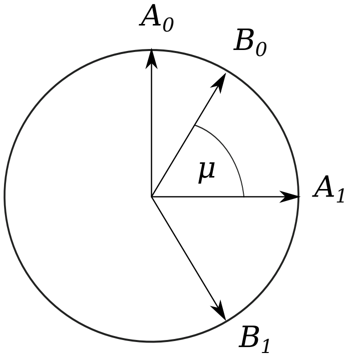

Figure 2.3: The optimal measurements for the maximal violation of the tilted CHSH inequality depicted on the XZ plane of the Bloch sphere with. Alice's measurements are Pauli's σ_X and σ_Z, while Bob's measurements are linear combinations of σ_X and σ_Z, symmetric around σ_X.

and it is realized with the following strategy

$$\begin{gathered} |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ A_i = s_i\sigma_X + c_i\sigma_Z, \quad B_i = s'_i\sigma_X + c'_i\sigma_Z. \end{gathered} \tag{2.15}$$

where $s_i = \sin\phi_i, c_i = \cos\phi_i, s'_i = \sin\phi'_i, c_i = \cos\phi'_i$, and $\phi_i = [(i-1)\pi]/n$ and $\phi'_i = [(2i-1)\pi]/2n$.

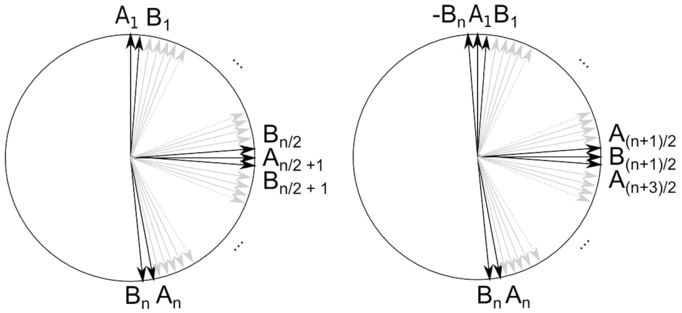

Figure 2.4: The optimal measurements for the maximal violation of the chained Bell inequality with n measurement inputs. The measurements are denoted with A_i and B_i and they are depicted on the XZ plane of the Bloch sphere with $i- = 1, \ldots, n$. The case with an even number of measurements is on the left, and the odd case is on the right.

Mermin inequality. The Bell inequality for three parties, related to the Greenberger-Horne-Zeilinger (GHZ) paradox [GHZ89, GHSZ90], is the Mermin inequality [Mer90]. The general form of the inequality is defined for any number of parties, denoted by $j =$

$\{1,\cdots,n\}$. Each party can measure one of two dichotomic observables, denoted by A_j and A'_j. The Mermin inequality reads:

$$\mathscr{I}^n_{Mer} = \frac{1}{2i}\left(\otimes^n_{j=1}(A_j + iA'_j) - \otimes^n_{j=1}(A_j - iA'_j)\right) \leq \begin{cases} 2^{n/2}, & \text{for even} \quad n; \\ 2^{(n-1)/2}, & \text{for odd} \quad n. \end{cases} \tag{2.16}$$

The maximum quantum violation is 2^{n-1} and it is achieved with the strategy

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + i\,|111\rangle), \\ A_j &= \sigma^j_{\mathrm{X}} \qquad A'_j = \sigma^j_{\mathrm{Y}}. \end{aligned} \tag{2.17}$$

2.2.4 Sum-of-squares (SOS) decompositions

To obtain a quantum violation of a bipartite Bell inequality two parties measure sets of quantum observables, denoted by $\{A_i\}$ and $\{B_j\}$ on a shared state ρ. In that case the Bell expression can be written in the following form

$$\mathscr{I} = \sum_{i,j} \tilde{b}_{i,j}\,\mathrm{tr}\left[A_i \otimes B_j \rho\right]$$

This expression can be equivalently written in terms of the Bell operator $\mathscr{B}$:

$$\mathscr{I} = \langle\mathscr{B}\rangle = \mathrm{tr}[\mathscr{B}\rho].$$

The Bell operator $\mathscr{B}$ can be expressed in terms of Alice's and Bob's measurement observables as $\sum_{i,j}\tilde{b}_{ij}A_i \otimes B_j$. If β_Q is the maximal quantum violation, the *shifted Bell operator* is defined as

$$\beta_Q\mathbb{1} - \mathscr{B}.$$

Since, by the very construction, this operator is positive-semidefinite, there exists a finite number of operators P_i (not necessarily positive) which are functions of the measurements A_i and B_i such that

$$\mathscr{B}_s = \beta_Q\mathbb{1} - \mathscr{B} = \sum_i P_i^\dagger P_i. \tag{2.18}$$

This decomposition is called a *sum-of-squares* (SOS) decomposition of the shifted Bell operator. Furthermore, an SOS decomposition in which operators P_i contain products of at most n measurement operators is named *SOS decomposition of n-th degree*. Numerically, it is possible to obtain SOS decompositions of various degrees via the Navascues-Pironio-Acin (NPA) hierarchy [NPA07]. In fact, the degree of the SOS decomposition is related to the level of the NPA hierarchy used. The dual of the semi-definite program defining the n-th level of the NPA hierarchy yields an SOS decomposition of n-th degree.

What is important for further considerations is that if $|\psi\rangle$ maximally violates some Bell inequality, then $(\beta_Q\mathbb{1} - \mathscr{B})\,|\psi\rangle = 0$, which implies that $P_i\,|\psi\rangle = 0$ for every i. In other words, $|\psi\rangle$ belongs to the intersection of kernels of the operators P_i. This imposes a plethora of conditions on the state and measurements maximally violating the Bell inequality.

2.3 Device-independence

As we saw in the previous section quantum entanglement is a necessary condition for Bell nonlocality. Consequently, the violation of a Bell inequality certifies the presence of entanglement in the system. Entanglement can also be verified directly, either by learning the state via tomographic methods or using an entanglement witness. The former method is more desirable, mostly because it requires less resources. Namely, for applying both state tomography and entanglement witness one needs a characterized measurement device, while Bell inequality violation can be observed with uncharacterized state source and measurement devices. All conclusions are drawn from the probability distribution $\{p(a,b|x,y)\}$, where the nature of inputs x,y and outputs a,b does not need to be specified. Thus, violation of a Bell inequality can be considered to be a *device-independent entanglement witness*. For any purpose the experimental devices can be treated as black-boxes. Such a scenario is not just a peculiar aspect of the foundations of quantum theory but an up-and-coming background for quantum information protocols.

Let us focus on quantum key distribution, one of the emblematic quantum information protocols. The highlight of quantum key distribution (QKD) is its utmost security. In other words, the security of QKD relies not on some complexity conjecture, but solely on the laws of physics. However, this security originally depended on the reliable physical implementation, which represented a weak spot exposed to eavesdroppers. The recovery of the unconditional security comes in virtue of the, aforementioned, device-independent paradigm. Device-independent quantum key distribution (DIQKD), establishes security directly from the probability distribution $\{p(a,b|x,y)\}$, assuming only validity of quantum mechanics, but dropping all assumptions about the physical operation of the devices. The main forebears of DIQKD are the early cryptographic result of Ekert [Eke91], the subsequent result of Barrett, Hardy and Kent [BHK05] and Mayers and Yao [MY04] pioneering work on self-testing. The first secure device-independent QKD protocol came out in 2007 [Aci+07], and it was the first time the term 'device-independent' was used.

The last ten years were fruitful in terms of device-independent quantum information processing. Let us itemize some of the main tasks, which can be performed in a device-independent manner

- witnessing the presence of entanglement;
- witnessing entangling measurement [Rab+11];
- quantum key distribution [Aci+07, VV14];
- quantum state certification - self-testing [MY04];
- randomness certification [AM16, Pir+10];
- testing the dimension of a Hilbert space [Bru+08].

2.4 Einstein-Podolsky-Rosen (EPR) steering

Another concept introduced in the early years of quantum theory, for a long time forgotten and revived with insurgence of quantum information theory is EPR-steering (or simply steering). It was described by Schrödinger in 1935, as a change of the quantum state of some particle induced by applying a local measurement on a spatially distant particle. In order for this to happen two particles must be entangled. In his work Schödinger was trying to formalize the idea already present in the seminal EPR paper. After entanglement and nonlocality, steering is the third type of quantum correlations we are discussing in this thesis and all three in some way originate from the famous EPR paper. Entanglement motivated the paradox, steering extended it, while nonlocality came as the answer to the paradox. Before passing to physical and operational differences and similarities between these three types of quantum correlations let us recall the revival of interest in steering, now understood as an important resource in quantum information theory. In 2007 Wiseman, Jones and Doherty reintroduced steering as a type of non-local correlations, incompatible with local hidden variable models [WJD07]. Since then steering has been scrutinized as an entanglement detection method, a resource for different quantum information protocols but also as an easy-to-handle tool for understanding other important fundamental concepts such as measurement incompatibility and Bell nonlocality.

The most basic EPR-steering scenario involves two parties, Alice and Bob, sharing some quantum state $\rho^{\mathrm{AB}} \in \mathbb{B}(\mathscr{H}^{\mathrm{A}} \otimes \mathscr{H}^{\mathrm{B}})$. Contrary to the Bell nonlocality scenario, the dimension of $\mathscr{H}^{\mathrm{B}}$ is fixed and known. Alice performs a measurement denoted by $x \in 0, \dots m-1$, by applying POVM $M_{a|x}$ on her share of the state. The measurement outcome is denoted by $a \in \{0, \dots o-1\}$. Following her measurement Bob's reduced state is

$$\sigma_{a|x} = \mathrm{tr}_{\mathrm{A}}[(M^{\mathrm{A}}_{a|x} \otimes \mathbb{1}^{\mathrm{B}})\rho^{\mathrm{AB}}].$$

Note that this state is subnormalized. The normalized state is obtained by adding a multiplication factor $1/p(a|x)$, where $p(a|x) = \mathrm{tr}[(M^{\mathrm{A}}_{a|x} \otimes \mathbb{1}^{\mathrm{B}})\rho^{\mathrm{AB}}]$ is a probability for Alice to obtain the outcome a when performing a measurement denoted by x. The set of subnormalized states $\{\sigma_{a|x}\}_{a,x}$ is called an *assemblage*. In accordance with the completeness of a POVMs $\sum_a M_{a|x} = \mathbb{1}$ the elements of an assemblage satisfy the following relation

$$\begin{aligned}\sum_a \sigma_{a|x} &= \mathrm{tr}_{\mathrm{A}}[(\sum_a M^{\mathrm{A}}_{a|x} \otimes \mathbb{1}^{\mathrm{B}})\rho^{\mathrm{AB}}] \\ &= \mathrm{tr}_{\mathrm{A}}[\rho^{\mathrm{AB}}] = \rho^{\mathrm{B}}, \qquad \forall x.\end{aligned}$$

Bob has access to a characterized measurement device and can learn all the elements of the assemblage. Steering represents a type of nonlocal correlations between Alice's measurement outcomes and the states prepared for Bob, i.e. elements of the corresponding assemblage. Recall that entanglement represents correlations between states of Alice and

Bob, while Bell nonlocality embodies the correlations between their measurement outcomes. In this sense, EPR-steering can be placed on a transition line between entanglement and nonlocality. Similarly, when considering entanglement of the state one knows dimensions of the local Hilbert spaces and the state is completely characterized, while on the other side of the spectra in the nonlocality scenario we make no assumptions about the dimensions of the local Hilbert spaces and do not characterize measurements either. Steering is again in the "transition region": one party has characterized measurement devices and a fixed Hilbert space dimension, while the other one functions in a black-box scenario. As nonlocality gave rise to the device-independent scenario, steering is native to the so-called *one-sided device-independent scenario*.

When are the correlations between Alice's measurement outcomes and the states prepared for Bob incompatible with classical predictions? Recall that an LHV model for nonlocality can be understood as a classical source sending classical messages, encoding the input-output relation, to both Alice ($p(a|x,\lambda)$) and Bob ($p(b|y,\lambda)$). Analogously, if the assemblage $\{\sigma_{a|x}\}$ is compatible with a source sending classical messages, encoding output-input relations to Alice ($p(a|x,\lambda)$) and quantum states to Bob (ρ_λ) we say that there is a *local hidden state* (LHS) model explaining it. An assemblage $\{\sigma_{a|x}\}$ admits an LHS model if:

$$\begin{aligned} \sigma_{a|x} &= \int d\lambda \mu_\lambda p(a|x,\lambda)\rho_\lambda, \qquad \forall a,x \\ &\int d\lambda \mu_\lambda = 1 \end{aligned} \tag{2.19}$$

If the assemblage $\{\sigma_{a|x}\}$ does not allow for the decomposition (2.19) it demonstrates steering. If Alice and Bob share a separable state ρ^{AB}, and Alice applies any POVM, the resulting assemblage will always have a decomposition (2.19). Note also that Alice and Bob are not symmetric in steering. We defined the problem here in the scenario where Alice is the untrusted and Bob the trusted party. Nothing forbids us to define the scenario with reversed roles. It has been proven that there are quantum states able to result in unsteerable assemblages when Alice is untrusted, but always leading to LHS assemblages when Bob is untrusted. This situation is known as one-way EPR-steering [BVQB14].

As there exist local entangled states, so do exist entangled states which can never demonstrate steering. These statea are called unsteerable. There are also states which can demonstrate steering, but cannot demonstrate nonlocality. Henceforth, entanglement, steering and nonlocality are all intrinsically different types of correlations [Qui+15].

There are two ways to detect steering: by using SDP optimizaiton and by violation of steering inequalities. For the end of this section we briefly discuss both methods.

- *SDP check.* Proving that an assemblage does not allow for a decomposition of the form (2.19) is in principle a very difficult task, because the hidden variable λ can have an infinite number of values. However, it can be proven that for a finite number of Alice's inputs and outputs, $p(a|x,\lambda)$ can be written as a convex combination of all different deterministic strategies

$$p(a|x,\lambda) = \sum_{\lambda'=1}^{d} p(\lambda'|\lambda) D(a|x,\lambda'), \tag{2.20}$$

where $d = o^m$. $D(a|x,\lambda')$ are strategies assigning a deterministic outcome to every measurement input. With this observation, the integral from (2.19) turns into a sum:

$$\sigma_{a|x} = \sum_{\lambda'=1}^{d} \tilde{\sigma}_{\lambda'} D(a|x,\lambda'), \qquad \forall a,x \tag{2.21}$$

where $\tilde{\sigma}_{\lambda'} = \int d\lambda \mu_\lambda p(\lambda'|\lambda)\rho_\lambda$. Now the problem of finding a decomposition of the form (2.21) can be cast as a SDP search:

$$\begin{aligned} \text{given} \quad & \{\sigma_{a|x}\}, \{D(a|x,\lambda)\} \\ \text{find} \quad & \{\tilde{\sigma}_\lambda\} \\ \text{s.t.} \quad & \sigma_{a|x} = \sum_{\lambda=1}^{d} \tilde{\sigma}_\lambda D(a|x,\lambda), \qquad \forall a,x \\ & \sigma_\lambda \geq 0, \qquad \forall \lambda. \end{aligned} \tag{2.22}$$

If $\{\tilde{\sigma}_\lambda\}$, satisfying above given constraints exists than the assemblage $\{\sigma_{a|x}\}$ is steerable. SDP (2.22) can be readily solved with some of the available SDP solvers.

- *Steering inequalities.* An analogue of Bell inequalities in the steering scenario are steering inequalities [CJWR09]. They can be trivially obtained as a reduction of Bell inequalities. For example, let us consider the situation when Alice can measure two dichotomic observables, denoted as A_0 and A_1. A natural reduction of CHSH inequality gives

$$\begin{gathered} \langle A_0 \otimes \frac{\sigma_Z + \sigma_X}{\sqrt{2}} \rangle + \langle A_1 \otimes \frac{\sigma_Z + \sigma_X}{\sqrt{2}} \rangle + \langle A_0 \otimes \frac{\sigma_Z - \sigma_X}{\sqrt{2}} \rangle - \langle A_1 \otimes \frac{\sigma_Z - \sigma_X}{\sqrt{2}} \rangle \leq 2 \\ \langle A_0 \otimes \sigma_Z \rangle + \langle A_1 \otimes \sigma_X \rangle \leq \sqrt{2} \end{gathered} \tag{2.23}$$

The maximal violation is achieved when Alice and Bob share the maximally entangled pair of qubits and when Alice measures $A_0 = \sigma_Z$ and $A_1 = \sigma_X$. Note that the violation of a steering inequality implies that Bob's assemblage admits for an LHS model, even without knowing the assemblage. Interestingly, the optimal steering inequalities for a given assemblage $\{\sigma_{a|x}\}$ which demonstrates steering can be obtained as a result of the dual formulation of SDP (2.22).

2.5 Self-testing

Self-testing is one of the simplest device-independent protocols. Introduced by Mayers and Yao [MY04], the standard self-testing scenario consists of a classical user who has access to several black boxes, which display some non-local correlations. The user received these boxes from a provider, who claims that to produce the observed correlations the boxes perform some specific measurements on a given quantum state. The goal of the classical user is to make sure that the boxes work properly, i.e. that they contain the claimed state and perform the claimed measurements. This is especially relevant if the user does not trust the provider or does not want to rely on the provider's ability to prepare the devices. Self-testing is the procedure that allows for this kind of certification. The self-tested states and measurements can later be used to run a given quantum information protocol, as proposed in [MY04] for secure quantum key distribution. For many protocols, however, passing through self-testing techniques is not necessary and in fact it is simpler and more efficient to run the protocol directly from the observed correlations, as for example in standard device independent quantum key distribution protocols [Aci+07]. Yet, self-testing protocols constitute an important device-independent primitive as they certify the entire description of the quantum setup only from the observed statistics.

As mentioned, the concept of self-testing was introduced by Mayers and Yao in [MY04], where the procedure to self-test a maximally entangled pair of qubits is described. This protocol was made robust in subsequent works, see [MYS14, Kan16]. In the following years new self-testing protocols for more complicated states such as graph states were described [McK14], as well as protocols for self-testing more complicated operations, such as entire quantum circuits [MMMO06]. A general numerical method for self-testing, known as the SWAP method, was introduced in [YVBSN14], providing exceptionally good robustness bounds. This numerical method can also be used to self-test three-qubit states such as GHZ states [PVN14] and W states [Wu+14]. The best analytical method for calculating robustness bound is presented in [Kan16].

Despite its importance, we lack general techniques to construct and prove self-testing protocols. Most of the existing examples are built from the maximal violation of a Bell inequality. Based on geometrical considerations, see for instance [FFW11, DPA13], one expects that generically there is a unique way, state and measurements, of producing the extremal correlations attaining the maximal quantum violation of a generic Bell inequality. This is not always the case, but whenever it is, we say that the corresponding Bell inequality is useful for self-testing. Following this approach, it is possible to prove that the state and measurements maximally violating the Clauser-Horne-Shimony-Holt (CHSH) inequality are unique, and the corresponding state is a maximally entangled two-qubit state. More recently, a self-testing protocol for any bipartite entangled state has been derived in [CGS17] extending the self-testing of all pure bipartite entangled two-qubit states [BP15]. From a general perspective, it is an interesting question to understand which Bell inequalities are useful for self-testing and what are the states and measurements certified by them.

2.5.1 Self-testing terminology

In this section we define the settings and introduce self-testing terminology. We consider the standard Bell scenario in which two parties share a quantum state $|\psi'\rangle$ on which they can perform n measurements, described by the two-outcome operators A'_j, B'_j , where $j = 1, ..., n$. The shared state and measurements are not trusted and are modelled as black boxes: each of them gets some classical input, which labels the choice of measurement, and produces a classical output, the measurement result. As the dimension is arbitrary, one can restrict the analysis to pure states and projective measurements without any loss of generality. The state $|\psi'\rangle$ lives in a joint Hilbert space $\mathscr{H}^{\mathrm{A}'} \otimes \mathscr{H}^{\mathrm{B}'}$ of an unknown dimension. Operators $A'_j(B'_j)$ act on the part of the state living in $\mathscr{H}'^{\mathrm{A}}(\mathscr{H}^{\mathrm{B}'})$, so that operators of different parties commute: $[A'_j, B'_k] = 0$. Also, $M^{\pm}_{A'_j} = (\mathbb{1} \pm A'_j)/2$ and $M^{\pm}_{B'_j} = (\mathbb{1} \pm B'_j)/2$ can be considered to be projective measurements. In this scenario the parties calculate the joint outcome probabilities that can be described as $p(a,b|j,k) = \langle\psi'| M^a_{A'_j} \otimes M^b_{B'_k} |\psi\rangle$. The parties can also check whether the probability distribution is non-local, i.e. whether some Bell inequality is violated.

Usually there is a specification of the black boxes, in self-testing terminology named as the *reference experiment*, and it consists of the state $|\psi\rangle \in \mathscr{H}^{\mathrm{A}} \otimes \mathscr{H}^{\mathrm{B}}$ and measurements A_j, B_j in some given Hilbert spaces $\mathscr{H}^{\mathrm{A}}$ and $\mathscr{H}^{\mathrm{B}}$ of finite dimension. On the other hand, the term *physical experiment* is used for the actual state and measurements $\{|\psi'\rangle, A'_j, B'_j\}$. The aim of self-testing is to compare the reference and the physical experiment and certify that they are physically equivalent. This means that the physical experiment is the same as the reference experiment up to local unitaries and additional non-relevant degrees of freedom, which are unavoidable, that is:

$$\begin{aligned} |\psi'\rangle &= U_{\mathrm{AA}_1} \otimes U_{\mathrm{BB}_1} |\psi\rangle_{\mathrm{AB}} |\mathrm{junk}\rangle_{\mathrm{A}_1\mathrm{B}_1} \\ A'_j \otimes B'_k |\psi'\rangle &= U_{\mathrm{AA}_1} \otimes U_{\mathrm{BB}_1} (A'_j \otimes B'_k |\psi\rangle_{\mathrm{AB}}) |\mathrm{junk}\rangle_{\mathrm{A}_1\mathrm{B}_1} \end{aligned}$$

where $|\mathrm{junk}\rangle_{\mathrm{A}_1\mathrm{B}_1}$ describe the local states of the possible additional degrees of freedom of the physical experiment and U_{AA_1} and U_{BB_1} are arbitrary local unitaries acting on systems AA_1 and BB_1. We introduce the product isometry $\Phi = \Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}} : \mathscr{H}^{\mathrm{A}'} \otimes \mathscr{H}^{\mathrm{B}'} \to \mathscr{H}^{\mathrm{A}} \otimes \mathscr{H}^{\mathrm{B}} \otimes \mathscr{H}^{\mathrm{A}_1} \otimes \mathscr{H}^{\mathrm{B}_1}$, a map that preserves the inner product, but does not have to preserve dimension. Thus we say that a self-testing protocol is successful if there exists a local isometry relating the physical and reference experiment:

$$\begin{aligned} \Phi(|\psi'\rangle) &= |\psi\rangle |\mathrm{junk}\rangle \\ \Phi(A'_j \otimes B'_k |\psi'\rangle) &= (A_j \otimes B_k |\psi\rangle) |\mathrm{junk}\rangle \end{aligned} \tag{2.24}$$

In self-testing terminology the relation between the physical and the reference experiment described by (2.24) is called *equivalence*. Trivially, a necessary condition for equivalence is that the full set of correlations obtained from the black boxes is equal to the set of correlations that one would obtain after applying the reference measurements on the reference state. A weaker necessary condition is to verify that the two sets of correlations lead to the same maximal quantum violation of a given Bell inequality. While in general checking all the correlations provides more information, there are some situations where observing just the maximum quantum value of a Bell inequality has been proven to be sufficient to certify the equivalence between the physical and the reference experiment.

The notion of equivalence, given above, captures the transformations which are physical and non-detrimental for the use of the underlying state in device-independent protocols, such as embedding the state in a larger Hilbert space, local changes of bases or appending ancillary degrees of freedom. However, it does not encompass complex conjugation of the state and measurements, a transformation which preserves the observed probabilities, but is not a physical transformation. In other words, the observed probability distributions can be obtained by an alternative realization not related with the ideal measurements by a local isometry. To remedy this, one can enlarge the set of transformations beyond local isometries in order to include complex conjugated measurements and states. In some parts of this thesis we use this enlarged set of transformations (local isometries + complex conjugation) as acceptable for self-testing. One of the open questions is if there are some more tranformations, not captured by local isometries, which should be included in the definition of self-testing.

2.5.2 Example: Self-testing via CHSH inequality

Self-testing of the maximally entangled pair of qubits via the maximal violation of CHSH inequality is probably the simplest and the most emblematic self-testing protocol. The reference experiment, i.e. the strategy which maximally violates the CHSH inequality is

$$\begin{gathered}
|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\
A_0 = \sigma_X, \qquad A_1 = \sigma_Z, \\
B_0 = \frac{\sigma_X + \sigma_Z}{\sqrt{2}}, \qquad B_1 = \frac{\sigma_X - \sigma_Z}{\sqrt{2}}.
\end{gathered}$$

Let is name this strategy the CHSH reference experiment. The CHSH operator is $\mathscr{B}_{CHSH} = A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1$ and the maximal violation achievable by the reference experiment is $2\sqrt{2}$. The SOS decomposition of the shifted CHSH operator is

$$2\sqrt{2}\mathbb{1} - \mathscr{B}_{CHSH} = \frac{1}{\sqrt{2}}\left[\left(A_0 - \frac{B_0 + B_1}{\sqrt{2}}\right)^2 + \left(A_1 - \frac{B_0 - B_1}{\sqrt{2}}\right)^2\right] \tag{2.25}$$

The above given operator vanishes on the state $|\psi'\rangle$ maximally violating CHSH inequality implying

$$\begin{aligned}
A_0|\psi'\rangle &= \frac{B_0+B_1}{\sqrt{2}}|\psi'\rangle, \\
A_1|\psi'\rangle &= \frac{B_0-B_1}{\sqrt{2}}|\psi'\rangle
\end{aligned} \tag{2.26}$$

These two relations in turn imply that operators A_0 and A_1 anticommute on the support of state $|\psi'\rangle$

$$\begin{aligned}
\{A_0,A_1\}|\psi'\rangle &= (A_0A_1+A_1A_0)|\psi'\rangle \\
&= A_0\frac{B_0-B_1}{\sqrt{2}}|\psi'\rangle + A_1\frac{B_0+B_1}{\sqrt{2}}|\psi'\rangle \\
&= \frac{B_0-B_1}{\sqrt{2}}\frac{B_0+B_1}{\sqrt{2}}|\psi'\rangle + \frac{B_0+B_1}{\sqrt{2}}\frac{B_0-B_1}{\sqrt{2}}|\psi'\rangle \\
&= \frac{B_0B_1-B_1B_0}{2}|\psi'\rangle + \frac{-B_0B_1+B_1B_0}{2}|\psi'\rangle \\
&= 0.
\end{aligned} \tag{2.27}$$

The explicitly constructed isometry is the SWAP gate [MYS14]. The operators used in the isometry are [1]

$$\begin{aligned}
X_\mathrm{A} &= A_1, \quad Z_\mathrm{A} = A_0, \\
X_\mathrm{B} &= \frac{B_0-B_1}{\sqrt{2}}, \quad Z_\mathrm{B} = \frac{B_0+B_1}{\sqrt{2}}.
\end{aligned}$$

The state of the system after applying the SWAP gate is

$$\begin{aligned}
\Phi(|\psi'\rangle) = |00\rangle &\frac{\mathbb{1}+Z_\mathrm{A}}{2}\frac{\mathbb{1}+Z_\mathrm{B}}{2}|\psi'\rangle \\
+|01\rangle &\frac{\mathbb{1}+Z_\mathrm{A}}{2}X_\mathrm{B}\frac{\mathbb{1}-Z_\mathrm{B}}{2}|\psi'\rangle \\
+|10\rangle &X_\mathrm{A}\frac{\mathbb{1}-Z_\mathrm{A}}{2}\frac{\mathbb{1}+Z_\mathrm{B}}{2}|\psi'\rangle \\
+|11\rangle &X_\mathrm{A}\frac{\mathbb{1}-Z_\mathrm{A}}{2}X_\mathrm{B}\frac{\mathbb{1}-Z_\mathrm{B}}{2}|\psi'\rangle
\end{aligned} \tag{2.28}$$

From eqs. (2.26) and (2.27) it follows that $Z_\mathrm{A}|\psi'\rangle = Z_\mathrm{B}|\psi'\rangle$, $X_\mathrm{A}|\psi'\rangle = X_\mathrm{B}|\psi'\rangle$, $\{X_\mathrm{A},Z_\mathrm{A}\}|\psi'\rangle = 0$ and $\{X_\mathrm{B},Z_\mathrm{B}\}|\psi'\rangle = 0$. Henceforth, $\frac{\mathbb{1}+Z_\mathrm{A}}{2}$ and $\frac{\mathbb{1}-Z_\mathrm{B}}{2}$ are orthogonal projectors and the

[1] Actually, regularized versions of X_B and Z_B are used in isometry, but we will describe in more details the regularization process in Chapter 3.

second and the third line of (2.28) vanish. Similarly the first and the fourth line simplify as follows

$$\begin{aligned} |00\rangle \frac{\mathbb{1}+Z_{\mathrm{A}}}{2}\frac{\mathbb{1}+Z_{\mathrm{B}}}{2}|\psi'\rangle &= |00\rangle \frac{\mathbb{1}+Z_{\mathrm{A}}}{2}|\psi'\rangle \\ |11\rangle X_{\mathrm{A}}\frac{\mathbb{1}-Z_{\mathrm{A}}}{2}X_{\mathrm{B}}\frac{\mathbb{1}-Z_{\mathrm{B}}}{2}|\psi'\rangle &= |11\rangle \frac{\mathbb{1}+Z_{\mathrm{A}}}{2}X_{\mathrm{A}}\frac{\mathbb{1}+Z_{\mathrm{B}}}{2}X_{\mathrm{B}}|\psi'\rangle \\ &= |11\rangle \frac{\mathbb{1}+Z_{\mathrm{A}}}{2}|\psi'\rangle \end{aligned}$$

Thus,

$$\Phi(|\psi'\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |\text{junk}\rangle \tag{2.29}$$

where $|\text{junk}\rangle = \frac{\mathbb{1}+Z_{\mathrm{A}}}{\sqrt{2}}|\psi'\rangle$, which is exactly the equivalence self-testing statement. Similarly, one can show that the SWAP gate maps physical measurement to the reference ones, as follows

$$\begin{aligned} \Phi(A_0|\psi'\rangle) &= \left[\sigma_{\mathrm{X}} \otimes \mathbb{1}\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right] \otimes |\text{junk}\rangle\,, \\ \Phi(A_1|\psi'\rangle) &= \left[\sigma_{\mathrm{Z}} \otimes \mathbb{1}\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right] \otimes |\text{junk}\rangle\,, \\ \Phi(B_0|\psi'\rangle) &= \left[\mathbb{1} \otimes \frac{\sigma_{\mathrm{X}} + \sigma_{\mathrm{Z}}}{\sqrt{2}}\frac{|00\rangle + |11\rangle}{\sqrt{2}})\right] \otimes |\text{junk}\rangle\,, \\ \Phi(B_1|\psi'\rangle) &= \left[\mathbb{1} \otimes \frac{\sigma_{\mathrm{X}} - \sigma_{\mathrm{Z}}}{\sqrt{2}}\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right] \otimes |\text{junk}\rangle\,, \end{aligned}$$

which completes the self-testing proof of the CHSH reference experiment.

2.6 Randomness from nonlocal correlations

The existence of intrinsic randomness is one of the big and debatable questions in modern science, technology and philosophy. Fundamentally, the notion of randomness is related to the important philosophical problems of determinism and free will. Practically, randomness is a resource for simulations, statistical sampling, cryptography, gambling and many others. It is one of the trademarks of quantum theory, in which outcomes of generic measurements can be predicted only probabilistically. Precisely this aspect motivated the EPR paradox, and subsequently Bell's theorem, which in turn brought a new light to the intrinsic randomness in quantum world. But before we explain the relation between Bell nonlocality and randomness let us explain what is meant by ”intrinsic”, or ”good” randomness.

Statement 1:
We say that N bits are random if they are unpredictable.

However, unpredictability depends on the context, since a sequence of numbers can be unpredictable for an observer, but perfectly predictable for another one, who possesses more information. A trivial example is dice throwing. The outcome is actually determined by Newton's laws and perfectly predictable with sufficient information. Thus, the statement about good randomness has to be modified.

Statement 2:
We say that N bits are random if there is no physical observer who can predict them.

Randomness defined in this way is also called private, since the user who generates it in privacy is sure that nobody knows the generated sequence. The next arising problem is the certification of randomness. To certify that a sequence of N bits is random means to prove that it is

- distributed according to the uniform distribution (i.e. both outcomes happen with the same probability);
- uncorrelated with the rest of the universe.

A quantum user, say Alice, can generate N random bits by measuring in $\{|0\rangle, |1\rangle\}$ basis the following state

$$\rho^{\mathrm{A}} = \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right)^{\otimes N}. \tag{2.30}$$

She can easily certify that the outcomes are distributed uniformly. However, Alice can have a reduced state identical to (2.30) but still be perfectly correlated with an eavesdropper, named Eve, if they share N maximally entangled pairs

$$|\psi\rangle^{\mathrm{AE}} = |\Phi^{+}\rangle^{\otimes N}. \tag{2.31}$$

A way for Alice to refute the possibility that Eve holds a system perfectly correlated with her is to prove that her system is maximally entangled with another system she has in possession. Due to the monogamy of entanglement, N pairs of maximally entangled qubits are uncorrelated with the rest of the universe. Since Alice obtains her bits one by one, we will consider a situation when $N = 1$. The rest of the bits are obtained by repeating the same protocol. Since Alice does not want to put any trust on the providers of her devices, she will operate in the device-independent scenario. Certifying that two of her boxes contain the maximally entangled pair of qubits can come through nonlocality. We have seen in Section 2.5 that the maximal violation of the CHSH inequality fixes the shared state and measurements to be equivalent to the EPR reference experiment. In other words, if Alice observes that her boxes achieve the Tsirelson bound in the CHSH scenario, she possesses a maximally entangled pair of qubits. A projective measurement on one of her qubits will produce a sequence of random numbers. The first protocol for device-independent randomness generation (DIRG) is given in [Pir+10], where it is shown how to quantify randomness. It provides a quantitative relation between the degree of violation of CHSH inequality and the amount of generated randomness.

The main task in a device independent randomness generation protocol is to estimate the ability of Eve to predict the outcomes of Alice's measurement, which is quantified by a quantity called *guessing probability*. Before defining the quantity, let us set the scenario. In a single-user protocol Alice possesses two boxes, A and B, which do not communicate. The state contained in the boxes can be correlated with Eve's system, and the joint state is denoted as $\rho^{\mathrm{ABE}} \in \mathbb{B}(\mathscr{H}^{\mathrm{A}} \otimes \mathscr{H}^{\mathrm{B}} \otimes \mathscr{H}^{\mathrm{E}})$. Analogously to the Bell test, Alice probes her boxes with classical inputs x and y, and obtains outcomes a and b, which are interpreted as the results of the measurements performed on a quantum state. By repeating the process, she evaluates the joint probabilities $p(a,b|x,y)$ and constructs a behaviour vector $\mathbf{P}$. The joint probabilities are obtained by the Born rule

$$p(a,b|x,y) = \mathrm{tr}\left[(M^{\mathrm{A}}_{a|x} \otimes M^{\mathrm{B}}_{b|y})\rho^{\mathrm{AB}}\right], \tag{2.32}$$

where $\rho^{\mathrm{AB}} = \mathrm{tr}_{\mathrm{E}}\rho^{\mathrm{ABE}}$.

The aim is to associate the guessing probability arising from the worst case quantum strategy compatible with $\mathbf{P}$. Let us focus on *local* randomness associated to Alice's input x^*. Upon Alice's measurement x^* the correlation between her output and Eve's state is captured by the quantum-classical state

$$\sum_a p(a|x^*)|a\rangle\langle a| \otimes \rho^{\mathrm{E}}_{a,x^*},$$

where

$$\rho^{\mathrm{E}}_{a,x^*} = \mathrm{tr}_{\mathrm{AB}}[(M^{\mathrm{A}}_{a|x^*} \otimes \mathbb{1}^{\mathrm{BE}})\rho^{\mathrm{ABE}}]$$

is the corresponding reduced state of Eve conditioned on Alice's outcome a. The guessing probability [CK11] is defined as the average probability that Eve correctly guesses Alice's output a. To guess the output Eve performs a POVM $\{M_{a|z}\}$ on her system. She guessed correctly if the outcome of her measurement is a when her system is in reduced state $\rho^{\mathrm{E}}_{a',x^*}$ which happens with probability

$$p(a|z,a',x^*) = \mathrm{tr}\left[M_{a|z}\rho^{\mathrm{E}}_{a,x^*}\right]. \tag{2.33}$$

The guessing probability is obtained by averaging (2.33) with respect to Alice's probability distribution $p(a|x^*)$ and optimizing over all possible POVMs Eve can perform and all quantum strategies compatible with the observed behaviour $\mathbf{P}$

$$G(\mathbf{P}) = \max_{M_{a|z},\mathrm{strat.}} \sum_a p(a|x^*)p(a|z,a',x^*). \tag{2.34}$$

There are several works dealing with the best ways to optimize the guessing probability, most notably [NSPS13, BSS14].

2.7 Semidefinite programming

A very common task in quantum information theory is to optimize some variable depending on a quantum state or a quantum behaviour. Examples of such variables are the maximal violation of a Bell inequality or a guessing probability. Since the sets over which the variable is optimized are often convex, such problems are usually solved by means of convex optimization methods. A particularly useful convex optimization tool in quantum information theory is semidefinite programming (SDP) [BV04]. Its aim is to optimize the value of an objective function over the intersection of the cone of positive semidefinite matrices and an affine space depending on the given constraints. Before presenting more details about semidefinite programming, let us recall a few definitions.

Matrix $\mathrm{M} \in M_n$ is *positive semidefinite* if $x^T \mathrm{M} x \geq 0$ for all vectors $x \in \mathbb{R}^n$. The following statements are equivalent:

- The matrix M is positive semidefinite.
- All eigenvalues of M are non-negative.
- All leading principal minors of M are non-negative.
- There exists N such that $\mathrm{M} = \mathrm{N}^T \mathrm{N}$.

A *convex cone* C is a subset of a vector space X, closed under linear combinations with positive coefficients. The *dual cone* C^* of a cone C is a subset of the dual vector space X^* defined by

$$C^* = \{y \in X^* | \langle y, x \rangle \geq 0, \forall x \in C\}.$$

We can now continue with the description of SDP optimizations. The simplest SDP optimization problem has the following primal formulation

$$\begin{aligned} \max_X \quad & \mathrm{tr}[AX]; \\ \text{s.t.} \quad & f(X) = B; \\ & X \geq 0, \end{aligned} \tag{2.35}$$

where A and B are Hermitian matrices, and f a hermicity-preserving linear map. Thus, the aim is to maximize the value of the *primal objective function* $\mathrm{tr}[AX]$ over the set of positive semidefinite operators satisfying *linear matrix equality* (LME) $f(X) = B$. All positive semidefinite operators X satisfying LME are named *primal feasible points*. If the set of primal feasible points is non-empty the SDP is feasible, otherwise it is infeasible. The maximal value of the primal objective function is named the *primal optimal value*.

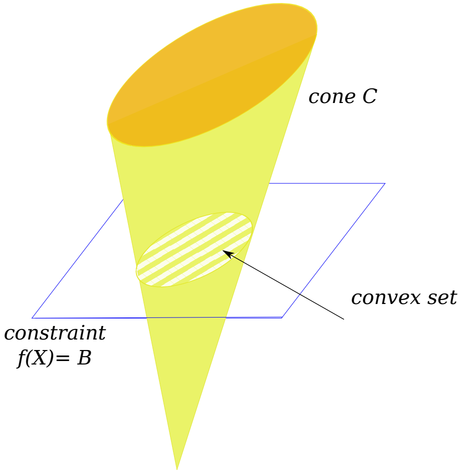

Figure 2.5: Representation of the cone C of positive semidefinite matrices. For a feasible SDP optimization problem the linear constraint $f(X) = B$ defines a plane which intersects the cone C, defining a convex set of all positive semidefinite matrices satisfying the constraint. The objective function is maximized over this convex set.

Every SDP can be written in its dual form. In order to find the dual form of the SDP given in (2.35) let us recall its associated Lagrangian

$$\begin{aligned} L &= \mathrm{tr}[AX] + \mathrm{tr}[Y(B - f(X))] + \mathrm{tr}[ZX] \\ &= \mathrm{tr}[(A - f^{\dagger}(Y) + Z)X] + \mathrm{tr}[BY], \end{aligned}$$

where Y and Z are Hermitian Lagrange multipliers corresponding to the two constraints of the primal problem. $f^{\dagger}$ is the conjugate map to f, defined by $\mathrm{tr}[f(X)Y] = \mathrm{tr}[Xf^{\dagger}(Y)]$ for all Hermitian X and Y. Note that $L \geq \mathrm{tr}[AX]$ whenever $Z \geq 0$, i.e. Lagrangian puts an upper bound on the primal optimal value. The Lagrangian has the smallest value when $Z = f^{\dagger}(Y) - A$. Henceforth, by imposing this condition and minimizing the remain of the Lagrangian over Lagrange multipliers we can obtain the lowest upper bound to the primal optimal value. This is exactly the dual formulation of the SDP

$$\begin{aligned} \min_{Y,Z} \quad & \mathrm{tr}[YB]; \\ \text{s.t.} \quad & Z + A = f^{\dagger}(Y); \\ & Z \geq 0. \end{aligned} \tag{2.36}$$

Z and Y are named *dual variables*, $\mathrm{tr}[YB]$ is the *dual objective function*, whose minimum is the *dual optimal value*. Operators satisfying $Z + A = f^{\dagger}(Y)$ are named dual feasible. Note that dual variable Z, also named a *slack variable*, can be eliminated from the dual, turning the remaining constraint into $f^{\dagger}(Y) - A \geq 0$. Thus, the dual can be simplified to the following form

$$\begin{aligned} \min_{Y,Z} \quad & \mathrm{tr}[YB]; \\ \text{s.t.} \quad & f^{\dagger}(Y) - A \geq 0. \end{aligned} \tag{2.37}$$

Denote by X^* and Y^* the primal and dual feasible point achieving the optimal primal value and optimal dual value, respectively. These points satisfy the following chain of relations

$$\mathrm{tr}\left[AX^*\right] \leq \mathrm{tr}\left[f^{\dagger}(Y^*)X^*\right] = \mathrm{tr}\left[Y^* f(X^*)\right] = \mathrm{tr}\left[Y^* B\right].$$

As noted earlier, these relations show that the primal optimal value is smaller than or equal to the dual optimal value, a concept known as the weak duality. The case of equality is known as the strong duality, and in that case the primal and dual SDP problems give the same value.

Part I

Device-independent certification of quantum states

Chapter 3

Self-testing protocols based on the chained Bell inequalities

In the previous chapter we introduced the idea of self-testing, outlined its importance for device-independent quantum information processing and explained relevant terminology. In this chapter we investigate self-testing properties of the chained Bell inequalities, defined in (2.14). More precisely, we show that by using the chained Bell inequalities one can self-test the maximally entangled state $|\Phi^+\rangle$ and certify the measurements given in (2.15). In this way we generalize the results previously obtained for the CHSH Bell inequality in Refs. [Tsi93, MYS14, MS12]. A significant aspect of our result is self-testing of measurements. While CHSH inequality one allows to self-test two anticommuting measurement observables, in the limit of a large n the chained Bell inequality allows one to self-test the entire plane of the Bloch sphere spanned by the Pauli matrices σ_X and σ_Z. Additionally, our results imply that the maximal quantum violation of the chained Bell inequalities is unique in the sense that there exists only one probability distribution maximally violating each of them. This makes chained Bell inequalities useful for randomness certification (see [DPA13]). In the context of nonlocal games this result confirms that measuring (2.15) on a maximally entangled state state $|\Phi^+\rangle$ is the only way (up to local isometries) to win the odd cycle game with maximal probability; it is known that the probability to win the odd-cycle game in the quantum regime is $\cos^2(\pi/4n)$ [CHTW04].

Before stating the technical results, let us set the scenario for the self-testing protocol. As in the standard Bell scenario, there are two parties, Alice and Bob, each in possession of a black box. The boxes contain shares of a quantum state $|\psi'\rangle$. Alice can apply one of n dichotomic measurements, corresponding to the measurement observable A_i. Similarly, Bob's measurement observables are denoted with B_i. In a way described in Section 2.2 Alice and Bob can gather data and calculate conditional probability distributions $p(a,b|x,y)$ and the corresponding correlators $\langle A_i B_j \rangle$. Recall that the chained Bell operator and the chained Bell inequality have the following form

$$\mathscr{B}_{ch}^{n} = \sum_{i=1}^{n} \left(A_i B_i + A_{i+1} B_i\right)$$
$$\mathscr{I}_{ch}^{n} = \langle \mathscr{B}_{ch}^{n} \rangle \leq 2n - 2.$$

The chapter is organized as follows. Section 3.1 introduces different SOS decompositions of the shifted chained Bell operators, which are used to prove the self-testing protocol described in Section 3.2. The consequences of noise and imperfect experimental measurements to the self-testing protocol are discussed in Section 3.3. Generation of randomness from the maximal violation of the chained Bell inequalities is the subject of Section 3.4. Finally, Section 3.5 concludes the chapter with the outlook and discussion about anticipated further work.

3.1 The SOS decompositions

The concept of SOS decompositions of a shifted Bell operators and their significance is outlined in Subsection 2.2.4. Two SOS decompositions of the shifted Bell operator associated to the chained Bell inequality are the main building block of our self-testing proof. We start from the first degree SOS decomposition.

Lemma 2.1. *Let $\{|\psi'\rangle, A_i', B_i'\}$ be the state and the measurements maximally violating the chained Bell inequality. Then, the corresponding shifted Bell operators admit the following SOS of first degree:*

$$\begin{aligned} \beta_Q^n \mathbb{1} - \mathscr{B}_{ch}^{n} \;\; = \;\; \cos\frac{\pi}{2n} \Bigg[& \sum_{i=1}^{n} \left(\mathbb{1} - A_i' \otimes \frac{B\_i + B_{i-1}'}{2\cos(\pi/2n)} \right)^2 \\ & + \frac{1}{n} \sum_{j=1}^{n} \sum_{i=1}^{n-2} \left(\alpha_i B_j' + \beta_i B_{i+j}' + \gamma_i B_{i+j+1}' \right)^2 \Bigg], \end{aligned} \tag{3.1}$$

where we assume that $B_{n+j}' = -B_j'$ and $B_n' = -B_0'$. The coefficients α_i, β_i, and γ_i are given by

$$\alpha_i = \frac{\sin(\pi/n)}{2\cos(\pi/2n)} \sqrt{\frac{1}{\sin(\pi i/n)\sin[\pi(i+1)/n]}}, \tag{3.2}$$

$$\beta_i = \frac{-1}{2\cos(\pi/2n)} \sqrt{\frac{\sin[\pi(i+1)/n]}{\sin(\pi i/n)}}, \tag{3.3}$$

and

$$\gamma_i = \frac{1}{2\cos(\pi/2n)} \sqrt{\frac{\sin(\pi i/n)}{\sin[\pi(i+1)/n]}} = -\frac{1}{4\beta_i \cos^2(\pi/2n)} \tag{3.4}$$

with $i = 1, \ldots, n-2$.

Before we prove this Lemma, note that the above SOS decomposition remains valid if in its second line we omit the sum over j and fix j to be any number from $\{1,\dots,n\}$. Also, the transformations $A_i' \to B_i'$ and $B_i' \to A_{i+1}'$ in the first parenthesis, and $B_i' \to A_i'$ in the second one lead to the whole new family of $2n$ SOS decompositions. Let us also mention that that the above SOS decomposition is a particular case of an SOS decomposition for a more general Bell inequality which is presented in Ref. [Sal+17] together with an analytical method used to derive it.

Proof. The first sum of the right hand side of eq. (3.1) contains all the terms forming the shifted Bell operator $\beta_Q^n \mathbb{1} - \mathscr{B}_{ch}^n$, but also some additional terms of the form $B_k B_{k+1}$. The second sum serves exactly to cancel out these additional terms from the first sum. The bottleneck of the SOS decomposition reduces to proving that the coefficient multiplying the identity operator $\mathbb{1}$ is exactly $2n\cos(\pi/2n)$. This coefficient reads

$$T = \cos\frac{\pi}{2n}\left[n + \frac{n}{2\cos^2(\pi/2n)} + T_\alpha + T_\beta + T_\gamma\right], \tag{3.5}$$

where

$$T_\omega = \sum_{i=1}^{n-2} \omega_i^2 \tag{3.6}$$

with $\omega = \alpha, \beta, \gamma$. The coefficients α_i, β_i and γ_i are defined in Eqs. (3.2), (3.3) and (3.4). In what follows we will evaluate each term T_ω separately. Let us start from T_α. Based on Eq. (3.2) we can write

$$\begin{aligned} T_\alpha \quad &= \tfrac{1}{4\cos^2(\pi/2n)} \textstyle\sum_{i=1}^{n-2} \left[\tfrac{\sin^2(\pi/n)}{\sin(i\pi/n)\sin[(i+1)\pi/n]}\right] \\ &= \tfrac{\sin(\pi/n)}{4\cos^2(\pi/2n)} \textstyle\sum_{i=1}^{n-2} \left[\tfrac{\cos(i\pi/n)}{\sin(i\pi/n)} - \tfrac{\cos[(i+1)\pi/n]}{\sin[(i+1)\pi/n]}\right] \\ &= \tfrac{\sin(\pi/n)}{4\cos^2(\pi/2n)} \textstyle\sum_{i=1}^{n-2} \left\{\cot\left(\tfrac{i\pi}{n}\right) - \cot\left[\tfrac{(i+1)\pi}{n}\right]\right\}. \end{aligned} \tag{3.7}$$

Note that the following identity

$$\sum_{i=1}^{n-1} \cot\left(\frac{\pi i}{n}\right) = 0 \tag{3.8}$$

implies

$$\sum_{i=1}^{n-2} \cot(\frac{i\pi}{n}) = \cot(\frac{\pi}{n}), \qquad \sum_{i=1}^{n-2} \cot(\frac{(i+1)\pi}{n}) = -\cot(\frac{\pi}{n}), \tag{3.9}$$

By plugging in Eq. (3.9) into Eq. (3.7) one can show that

$$T_\alpha = \frac{\cos(\pi/n)}{2\cos^2(\pi/2n)}. \tag{3.10}$$

Let us, now, evaluate T_β. Following Eq. (3.3), T_β takes the following form

$$T_\beta = \frac{1}{4\cos^2(\pi/2n)}\left[\sum_{i=1}^{n-2}\frac{\sin[(i+1)\pi/n]}{\sin(i\pi/n)}\right]. \tag{3.11}$$

After utilizing the elementary trigonometric property $\sin(x+y) = \sin x\cos y + \cos x\sin y$, Eq. (3.11) reduces to

$$T_\beta = \frac{1}{4\cos^2(\pi/2n)}\left[(n-2)\cos(\frac{\pi}{n}) + \sin(\frac{\pi}{n})\sum_{i=1}^{n-2}\cot(\frac{i\pi}{n})\right]. \tag{3.12}$$

Finally, by aid of Eq. (3.9), this gives

$$T_\beta = \frac{(n-1)\cos(\pi/n)}{4\cos^2(\pi/2n)}. \tag{3.13}$$

Let us finally compute T_γ. From Eq. (3.4) it can be written explicitly as

$$T_\gamma = \frac{1}{4\cos^2(\pi/2n)}\left[\sum_{i=1}^{n-2}\frac{\sin(i\pi/n)}{\sin[(i+1)\pi/n]}\right]. \tag{3.14}$$

If we write $\sin(i\pi/n) = sin[(i+1-1)\pi/n]$ and use again the above given trigonometric identity, one finds

$$T_\gamma = \frac{1}{4\cos^2(\pi/2n)}\left\{(n-2)\cos(\frac{\pi}{n}) - \sin(\frac{\pi}{n})\sum_{i=1}^{n-2}\cot\left[\frac{(i+1)\pi}{n}\right]\right\}, \tag{3.15}$$

which, following Eq. (3.9), reduces to

$$T_\gamma = \frac{(n-1)\cos(\pi/n)}{4\cos^2(\pi/2n)}. \tag{3.16}$$

At the end, if we plug-in Eqs. (3.10), (3.13) and (3.16) into Eq. (3.5) and exploit some elementary properties of the trigonometric functions, we can see that $T = 2n\cos(\pi/2n)$, which completes the proof. □

While useful for gaining knowledge about $|\psi'\rangle$ and operators $\{A'_i, B'_i\}$, the SOS decomposition (3.1) does not provide enough informations for self-testing. To remedy this, we have to introduce a 2nd degree SOS decomposition.

Lemma 2.2. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ be the state and the measurements maximally violating the chained Bell inequality. Then, the corresponding shifted Bell operator admits the* *following second-order SOS:*

$$\beta_Q^n\mathbb{1}-\mathscr{B}_{ch}^n=\frac{1}{8n\cos\frac{\pi}{2n}}\Bigg\{2(\beta_Q^n\mathbb{1}-\mathscr{B}_{ch}^n)^2+\sum_{\substack{i,j=1\\ j\neq i,i-1}}^{n}\left[A_i'\otimes(B_i'+B_{i-1}')-(A_j'+A_{j+1}')\otimes B_j'\right]^2$$
$$+\sum_{i=1}^{n}\left[\left(A_i'\otimes B_i'-A_{i+1}'\otimes B_{i+1}'\right)^2+\left(A_i'\otimes B_{i-1}'-A_{i+1}'\otimes B_i'\right)^2\right]\Bigg\}$$
$$+\frac{1}{2}\cos\left(\frac{\pi}{2n}\right)\sum_{i=1}^{n-2}\left[\left(\alpha_iB_1'+\beta_iB_{i+1}'+\gamma_iB_{i+2}'\right)^2+\left(\alpha_iA_1'+\beta_iA_{i+1}'+\gamma_iA_{i+2}'\right)^2\right], \tag{3.17}$$

where we again used the notation $A_{n+1}'=-A_1'$ and $A_0'=-A_n'$ and the same for B'-s, and the α_i, β_i and γ_i are given in Eqs. (3.2), (3.3) and (3.4).

We can construct another SOS decomposition from the above one by applying the following transformations to it: $A_i'\to B_i'$ in all terms, $B_i'\to A_{i+1}'$ in the curly brackets and $B_i'\to A_i'$ in the remaining terms.

Proof. To confirm validity of (3.17) we follow similar argumentation as in the proof of Lemma 2.1. The first parenthesis on the right hand side of (3.17) introduces terms that up to some multiplicative factors belong to the following set $\{\ \mathbb{1}, A_i'B_i', A_i'B_{i-1}', A_i'A_{i+1}', B_i'B_{i+1}', A_i'A_j'B_k'B_l'\}$. The terms $A_i'A_j'B_k'B_l'$ are directly cancelled out by the same terms stemming from the second and the third parenthesis. Then, the terms $A_i'A_{i+1}'$ and $B_i'B_{i+1}'$ enter with the coefficient $2/[8n\cos(\pi/2n)]$ and together with the same terms resulting from the second parenthesis and entering with the coefficient $(n-2)/[8n\cos(\pi/2n)]$ they are cancelled out by those resulting from the third line of (3.17). The terms $A_i'B_i'$ and $A_i'B_{i-1}'$ give rise to the shifted Bell operator, and, finally, the identity operator $\mathbb{1}$ is multiplied by the following expression

$$\frac{1}{8n\cos(\pi/2n)}\left\{\left[8n^2\cos^2(\frac{\pi}{2n})+4n\right]+4n(n-2)+4n\right\}+\frac{n\cos(\pi/n)}{2\cos^2(\pi/2n)} \tag{3.18}$$

which after some movements simplifies to $2n\cos(\pi/2n)$. This is exactly the multiplicative factor of identity operator in the shifted Bell operator. □

3.2 Exact case self-testing

In this Section we consider the situation when a chained Bell inequality is maximally violated and prove that it has a strong self-testing consequences. The starting point is the swap-gate introduced in Ref. [McKM11] and presented on Fig. 3.1. In what follows we will demonstrate that with adequately chosen operators X_A', Z_B', X_B' and Z_B' it defines a

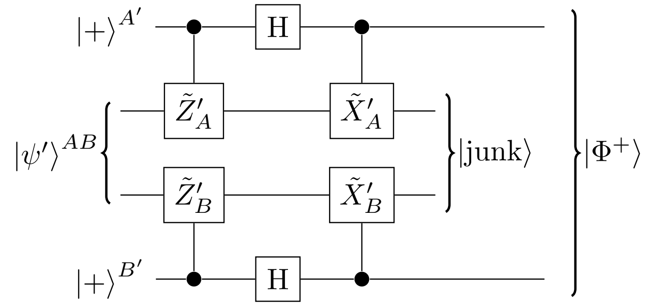

Figure 3.1: The swap-gate used for self-testing. In it, $|\psi'\rangle^{AB}$ stands for the state maximally violating the given Bell inequality, while $|+\rangle^{A'}$ and $|+\rangle^{B'}$ are ancillary qubit states controlling the gates $\tilde{X}_A$,$\tilde{Z}_A$,$\tilde{X}_B$ and $\tilde{Z}_B$. Then, H is the standard one-qubit Hadamard gate defined in the text. $\tilde{X}_A$,$\tilde{Z}_A$,$\tilde{X}_B$ and $\tilde{Z}_B$ are regularized, if necessary, versions of X'_A,Z'_A,X'_B and Z'_B respectively. At the output of the circuit the ancillary qubits are in the desired state $|\Phi_+\rangle$.

unitary operation satisfying Eq. (2.24), necessary for self-testing. For this purpose, let us choose

$$X'_A = \begin{cases} A'_{n/2+1}, & n \text{ even} \\[2ex] \dfrac{A'_{(n+1)/2}+A'_{(n+3)/2}}{2\cos(\pi/2n)}, & n \text{ odd} \end{cases}, \qquad Z'_A = A_1 \tag{3.19}$$

and

$$X'_B = \begin{cases} \dfrac{B'_{n/2}+B'_{n/2+1}}{2\cos(\pi/2n)}, & n \text{ even} \\[2ex] B_{(n+1)/2}, & n \text{ odd} \end{cases}, \qquad Z'_B = \frac{B'_1 - B'_n}{2\cos(\pi/2n)}. \tag{3.20}$$

Since all observables A'_i and B'_i are Hermitian with eigenvalues ± 1, Z'_A and X'_A for even n and X'_B for odd n are unitary. Yet, the operators X'_A for odd n, X'_B for even n and Z'_B may not be unitary, making the swap-gate possibly non-unitary. This problem is solved by utilizing the polar decomposition which says that any operator M can be written as $M = U|M| = |M|V$ where U and V are some unitary operators and $|M| = \sqrt{M^\dagger M}$. If X'_B and Z'_B are of full rank let us define $\widetilde{X}_B = X'_B/|X'_B|$ and $\widetilde{Z}_B = Z'_B/|Z'_B|$, while if any of them is rank deficient, say Z'_B, we replace its zero eigenvalues by one and then use the above construction. To sum up, we define $\widetilde{Z}_B = (Z'_B + P)/|Z'_B + P|$ where P denotes the projector onto the kernel of Z'_B.

Now, note that the SOS decompositions (3.1) and (3.17) imply that for any $i = 1, \ldots, n$ the identities

$$A'_i \otimes \frac{B'_i + B'_{i-1}}{2\cos(\pi/2n)} |\psi'\rangle = |\psi'\rangle, \qquad \frac{A'_i + A'_{i+1}}{2\cos(\pi/2n)} \otimes B_i |\psi'\rangle = |\psi'\rangle \tag{3.21}$$

are satisfied, which further entail that

$$X'_A\,|\psi'\rangle = X'_B\,|\psi'\rangle\,, \qquad Z'_A\,|\psi'\rangle = Z'_B\,|\psi'\rangle\,. \tag{3.22}$$

Furthermore, one can prove the anticommutation of operators X'_A and Z'_A on the support of $|\psi'\rangle$

$$\{X'_A, Z'_A\}\,|\psi'\rangle = 0. \tag{3.23}$$

To demonstrate this relation we need to prove several auxiliary lemmas. Before we proceed let us note that in some of the following expressions operators might be indexed by any integer (not just from the set $\{1,\ldots,n\}$), and in those cases we use the notation $C_{n+i} = -C_i$ and $C_{-i} = -C_{n-i}$. The intuition for this notation can be found on Bloch sphere representation of the measurements (see Fig. 2.4), where we can see that if one would draw the next measurement after C_n, and denote it as C_{n+1} it would be parallel to $-C_1$, and similarly for any C_{n+i}. Let us continue by proving the following lemma.

Lemma 2.3. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ be the pure state and the measurements realizing the maximal quantum violation of the chained Bell inequalities. Then, the following identities are true:*

$$A'_i\,|\psi'\rangle = \frac{B'_i + B'_{i-1}}{2\cos(\pi/2n)}\,|\psi'\rangle \equiv B'_{i-1,i}\,|\psi'\rangle \tag{3.24}$$

for $i = 1,\ldots,n$,

$$(\alpha_i C_j + \beta_i C_{i+j} + \gamma_i C_{i+j+1})\,|\psi'\rangle = 0 \tag{3.25}$$

for $i = 1,\ldots,n-2$, $j = 1,\ldots,n$ and $C = A', B'$, and

$$(A'_i B'_i - A'_{i+1} B'_{i+1})\,|\psi'\rangle = 0 \tag{3.26}$$

$$(A'_i B'_{i-1} - A'_{i+1} B'_i)\,|\psi'\rangle = 0 \tag{3.27}$$

for $i = 1,\ldots,n$.

Proof. From the fact that $|\psi'\rangle$ and A'_i and B'_i violate the chained Bell inequality maximally it follows that $\langle\psi'|(\beta^n_Q \mathbb{1} - \mathscr{B}^n_{ch})\,|\psi'\rangle = 0$. Now, the first SOS decomposition (3.1) for the operator $\beta^n_Q \mathbb{1} - \mathscr{B}^n_{ch}$ implies Eqs. (3.24) and (3.25), while the second one implies Eqs. (3.26) and (3.27) □

This Lemma together with the following one is enough to prove the anticommutation relation (3.23).

Lemma 2.4. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ be the pure state and the measurements realizing the maximal quantum violation of the chained Bell inequalities. Then, the following relations are true:*

$$\{A'_1, A'_{\frac{n}{2}+1}\}\,|\psi'\rangle = 0 \tag{3.28}$$

for even n, and

$$\{A'_1, A'_{\frac{n+1}{2}} + A'_{\frac{n+3}{2}}\}\,|\psi'\rangle = 0 \tag{3.29}$$

for odd n.

Proof. We prove the even and odd n case separately.

Even number of measurements. Let us begin by noting that by setting $j = k - i$ with $k = 1, \ldots, n$ in (3.25), one obtains

$$(\alpha_i C_{k-i} + \beta_i C_k + \gamma_i C_{k+1})\,|\psi'\rangle = 0. \tag{3.30}$$

Alternatively, by shifting $i \to n - i - 1$ and fixing $j = k + i + 1$, we get

$$(\alpha_{n-i-1} C_{k+i+1} + \beta_{n-i-1} C_{k+n} + \gamma_{n-i-1} C_{k+n+1})\,|\psi'\rangle = 0, \tag{3.31}$$

which, by noting that $C_{k+n} = -C_k$ for any $k = 1, \ldots, n-1$, $\alpha_{n-i-1} = \alpha_i$ and $\beta_{n-i-1} = -\gamma_i$ for any $i = 1, \ldots, n-2$, can further be simplified to

$$(\alpha_i C_{k+i+1} + \gamma_i C_k + \beta_i C_{k+1})\,|\psi'\rangle = 0. \tag{3.32}$$

After summing Eqs. (3.30) and (3.32) and performing some straightforward manipulations we finally obtain

$$(C_{k-i} + C_{k+i+1})\,|\psi'\rangle = \xi_i C_{k,k+1}\,|\psi'\rangle\,, \tag{3.33}$$

where we denoted $\xi_i = 2\cos[(2i+1)\pi/2n]$ and $C_{k,k+1} = (C_k + C_{k+1})/[2\cos(\pi/2n)]$. Finally, setting $k = 0$ in Eq. (3.32) and $k = n$ in Eq. (3.30) and subtracting the resulting equations one from another we obtain

$$(C_{i+1} - C_{n-i})\,|\psi'\rangle = \xi_i C_{1,-n}\,|\psi'\rangle\,, \tag{3.34}$$

where we have denoted $C_{1,-n} = (C_1 - C_n)/[2\cos(\pi/2n)]$.

Having all these auxiliary identities at hand, we are now in position to prove Eq. (3.28). To this end, we first rewrite its left-hand side as

$$\begin{aligned}(A'_1 A'_{\frac{n}{2}+1} + A'_{\frac{n}{2}+1} A'_1)\,|\psi'\rangle &= \left(A'_1 B'_{\frac{n}{2},\frac{n}{2}+1} + A'_{\frac{n}{2}+1} B'_{1,-n}\right)|\psi'\rangle \\ &= \frac{1}{\xi_{\frac{n}{2}-1}}\left[A'_1(B'_1 + B'_n) + A'_{\frac{n}{2}+1}(B'_{\frac{n}{2}} - B'_{\frac{n}{2}+1})\right]|\psi'\rangle\,,\end{aligned} \tag{3.35}$$

where the first equality was obtained with the aid of the identity (3.24) for $i = n/2 + 1$, while the second one follows from Eqs. (3.33) and (3.34). Then, the formulas (3.26) and (3.27) imply that

$$(A'_1 B'_1 - A'_{j+1} B'_{j+1})\,|\psi'\rangle = \sum_{i=1}^{j} (A'_i B'_i - A'_{i+1} B'_{i+1})\,|\psi'\rangle = 0 \tag{3.36}$$

and

$$(A'_1 B'_n + A'_{j+1} B'_j)\,|\psi'\rangle = \sum_{i=1}^{j} (A'_i B'_{i-1} - A'_{i+1} B'_i)\,|\psi'\rangle = 0 \tag{3.37}$$

hold for any $j = 1, \dots, n$. After setting $j = n/2$ in the latter identities and inserting them into Eq. (3.35) we eventually obtain (3.28).

Odd number of measurements. Before passing to the anticommutation relation (3.29), we need some auxiliary relations for the measurements A'_i and B'_i. In order to derive the first one, we shift $k \to k-1$ in Eq. (3.32) and add the resulting equation to Eq. (3.30), obtaining

$$(C_{k+i} + C_{k-i})\,|\psi'\rangle = -2\frac{\beta_i}{\alpha_i}C_k - \frac{\gamma_i}{\alpha_i}(C_{k-1} + C_{k+1})\,|\psi'\rangle\,. \tag{3.38}$$

Then, setting $i = 1$ and shifting $j \to j-1$ in Eq. (3.25) we arrive at

$$(C_{j+1} + C_{j-1})\,|\psi'\rangle = 2\cos\left(\frac{\pi}{n}\right)C_j\,|\psi'\rangle\,, \tag{3.39}$$

which after being plugged into Eq. (3.38) gives rise to the following identity

$$(C_{k+i} + C_{k-i})\,|\psi'\rangle = \zeta_i C_k\,|\psi'\rangle\,, \tag{3.40}$$

where $\zeta_i = 2\cos(i\pi/n)$.

Then, by setting $j = (n-1)/2$ in Eqs. (3.36) and (3.37) and adding the resulting equations we obtain

$$A'_1(B'_1 + B'_n)\,|\psi'\rangle = A'_{\frac{n+1}{2}}(B'_{\frac{n+1}{2}} - B'_{\frac{n-1}{2}})\,|\psi'\rangle\,, \tag{3.41}$$

which can be further simplified by using Eq. (3.40) with $i = (n-1)/2$ and $k = n$, giving

$$A'_1(B'_1 + B'_n)\,|\psi'\rangle = \zeta_{\frac{n-1}{2}}A'_{\frac{n+1}{2}}B'_n\,|\psi'\rangle\,. \tag{3.42}$$

Analogously, by setting $j = (n+1)/2$ in Eqs. (3.36) and (3.37) and adding them, one obtains

$$A'_1(B'_1 + B'_n)\,|\psi'\rangle = A'_{\frac{n+3}{2}}(B'_{\frac{n+3}{2}} - B'_{\frac{n+1}{2}})\,|\psi'\rangle\,, \tag{3.43}$$

which, after application of Eq. (3.40) with $i = (n-1)/2$ and $k = n+1$, further simplifies to

$$A'_1(B'_1 + B'_n)\,|\psi'\rangle = -\zeta_{\frac{n-1}{2}}A'_{\frac{n+3}{2}}B'_1\,|\psi'\rangle\,. \tag{3.44}$$

Now, we can rewrite the left-hand side of the anticommutation relation Eq. (3.29) as

$$\begin{aligned}
&\left\{A'_1, A'_{\frac{n+1}{2}} + A'_{\frac{n+3}{2}}\right\}|\psi'\rangle = \\
&\quad = \frac{1}{2\cos\frac{\pi}{2n}}\left[A'_1(B'_{\frac{n-1}{2}} + 2B'_{\frac{n+1}{2}} + B'_{\frac{n+3}{2}}) + (A'_{\frac{n+1}{2}} + A_{\frac{n+3}{\prime}2})(B'_1 - B'_n)\right]|\psi'\rangle \\
&\quad = \frac{1}{2\cos\frac{\pi}{2n}}\left[A'_1\left(B'_{\frac{n-1}{2}} + B'_{\frac{n+3}{2}} + 2\frac{B'_1 + B'_n}{\zeta_{(n-1)/2}}\right) + (A'_{\frac{n+1}{2}} + A'_{\frac{n+3}{2}})(B'_1 - B'_n)\right]|\psi'\rangle\,,
\end{aligned}$$

where the first equality stems from Eq. (3.24) and to obtain the second one we have utilized Eq. (3.40) with $i = (n-1)/2$ and $k = (n+1)/2$. Then, expressions (3.42) and (3.44) lead us to

$$\left\{A_1', A'_{\frac{n+1}{2}} + A'_{\frac{n+3}{2}}\right\}|\psi'\rangle = \frac{1}{2\cos(\pi/2n)}(A_1'B'_{\frac{n-1}{2}} + A_1'B'_{\frac{n+3}{2}} + A'_{\frac{n+1}{2}}B_1' - A'_{\frac{n+3}{2}}B_n')|\psi'\rangle\,. \tag{3.45}$$

Exploiting once more Eq. (3.40) one obtains the following equalities

$$A_1'|\psi'\rangle = \frac{1}{\zeta_{\frac{n-1}{2}}}(A'_{\frac{n+1}{2}} - A'_{\frac{n+3}{2}})|\psi'\rangle\,, \quad B_1'|\psi'\rangle = \frac{1}{\zeta_{\frac{n-1}{2}}}(B'_{\frac{n+1}{2}} - B'_{\frac{n+3}{2}})|\psi'\rangle\,,$$

and

$$B_n'|\psi'\rangle = \frac{1}{\zeta_{\frac{n-1}{2}}}(B'_{\frac{n+1}{2}} - B'_{\frac{n-1}{2}})|\psi'\rangle$$

whose application to Eq. (**??**) allows one to rewrite it as

$$\begin{aligned}\left\{A_1', A'_{\frac{n+1}{2}} + A'_{\frac{n+3}{2}}\right\}|\psi'\rangle = \\ = \frac{1}{2\zeta_{\frac{n-1}{2}}\cos\frac{\pi}{2n}}\left(A'_{\frac{n+1}{2}}B'_{\frac{n-1}{2}} - A'_{\frac{n+3}{2}}B'_{\frac{n+1}{2}} + A'_{\frac{n+1}{2}}B'_{\frac{n+1}{2}} - A'_{\frac{n+3}{2}}B'_{\frac{n+3}{2}}\right)|\psi'\rangle\,.\end{aligned}$$

To complete the proof it suffices to make use of the equalities (3.26) and (3.27) with $j = (n+1)/2$. □

Finally, although the tilded operators are in general different than X_B' and Z_B', it turns out that they act in the same way when applied to $|\psi'\rangle$, that is,

$$\widetilde{X}_B|\psi'\rangle = X_B'|\psi'\rangle\,, \qquad \widetilde{Z}_B|\psi'\rangle = Z_B'|\psi'\rangle\,. \tag{3.46}$$

To prove these relations, let $\|\cdot\|$ stand for the vector norm defined as $\|\,|\psi\rangle\,\| = \sqrt{\langle\psi|\psi\rangle}$. Then, the following reasoning applies (based on the metod from Ref. [BP15])

$$\begin{aligned}\|(\widetilde{X}_B - X_B')|\psi'\rangle\| &= \|(\mathbb{1} - \widetilde{X}_B^\dagger X_B')|\psi'\rangle\| = \|(\mathbb{1} - |X_B'|)|\psi'\rangle\| \\ &= \|(\mathbb{1} - |X_A'X_B'|)|\psi'\rangle\| \leq \|(\mathbb{1} - X_A'X_B')|\psi'\rangle\| = 0,\end{aligned} \tag{3.47}$$

where the first and the second equalities stem from the fact that $\widetilde{X}_B$ is unitary and its definition, respectively. The third equality is a consequence of the fact X_A' is unitary which implies that $|X_A'X_B'| = |X_B'|$, and, finally, the inequality and the last equality follow from the operator inequality $M \leq |M|$ and Eq. (3.22).

The following lemma is necessary for self-testing of all the measurements used to obtain the maximal violation of any of the chained Bell inequalities.

Lemma 2.5. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ realize the maximal quantum violation of the chained Bell inequality. Then, for even n:*

$$A'_i|\psi'\rangle = \left(s_iA'_{\frac{n}{2}+1} + c_iA'_1\right)|\psi'\rangle, \tag{3.48}$$

$$B'_i|\psi'\rangle = \left(s'_iB'_{\frac{n}{2},\frac{n}{2}+1} + c'_iB'_{1,-n}\right)|\psi'\rangle, \tag{3.49}$$

while for odd n:

$$A'_i|\psi'\rangle = \left\{s_iA'_{\frac{n+1}{2},\frac{n+3}{2}} + c_iA'_1\right\}|\psi'\rangle, \tag{3.50}$$

$$B'_i|\psi'\rangle = \left\{s'_iB'_{\frac{n+1}{2}} + c'_iB'_{1,-n}\right\}|\psi'\rangle, \tag{3.51}$$

are valid for any $i = 1,\dots,n$. Symbols s_i, c_i, s'_i and c'_i are defined in Eq. (2.15).

Proof. Let us begin with the even n case. By setting $k = 1 + n/2$ and shifting $i \to 1 - i + n/2$ in Eq. (3.40) one obtains

$$(C_i - C_{2-i})|\psi'\rangle = \zeta_{\frac{n}{2}+1-i}C_{\frac{n}{2}+1}|\psi'\rangle. \tag{3.52}$$

for $i = 1,\dots,n/2$, where we have additionally exploited the fact that $C_{n+i} = -C_i$ and $C_{-i} = -C_{n-i}$ for any i. To prove Eq. (3.52) for $i = n/2+1,\dots,n/2$ one has to use (3.30) but coefficients α_i, β_i and γ_i are not defined for $i < 0$. However, once Eq. (3.52) is derived for $i < n/2+1$, it is easy to note that the cases when $i > n/2+1$ are already contained in the proof. This is due to the fact that any expression obtained when $i > n/2+1$, is the same as the expression proved for $n+2-i < n/2+1$.

On the other hand, fixing $k = 1$ and shifting $i \to i-1$ in Eq. (3.40), one can deduce the following equality

$$(C_i + C_{2-i})|\psi'\rangle = \zeta_{i-1}C_1|\psi'\rangle. \tag{3.53}$$

with $i = 2,\dots n$. For $i = 1$ the equation is trivial. Adding Eqs. (3.52) and (3.53) and recalling that $\zeta_i = 2\cos(i\pi/n)$ one obtains Eq. (3.48).

In order to prove the second identity (3.49), we fix $k = n/2$ and shift $i \to n/2 - i$ in Eq. (3.33) which leads us to

$$(C_i + C_{n-i+1})|\psi'\rangle = \xi_{\frac{n}{2}-i}C_{\frac{n}{2},\frac{n}{2}+1}|\psi'\rangle. \tag{3.54}$$

This equation is satisfied for all $i = 1,\dots,n$, but it could formally be derived only when $i < n/2$. The cases $i = n/2, n/2+1$ are trivially satisfied. Similarly to the discussion following Eq. (3.52) it is easy to check that for every $i > n/2+1$ Eq. (3.54) is the same as for the case $n+1-i < n/2$, which has been formally proven.

Now we note that by shifting $i \to i-1$ in Eq. (3.34), one obtains the following equation

$$(C_i - C_{n-i+1})|\psi'\rangle = \xi_{i-1}C_{1,-n}|\psi'\rangle, \tag{3.55}$$

which when combined with Eq. (3.54) directly implies Eq. (3.49), completing the proof.

Now we move to the odd n case. First in Eq. (3.33) we fix $k = (n+1)/2$ and shift $i \to (n+1)/2 - i$ to get

$$(C_i + C_{n+2-i}) |\psi'\rangle = \xi_{\frac{n+1}{2}-i} C_{\frac{n+1}{2},\frac{n+3}{2}} |\psi'\rangle \, . \tag{3.56}$$

This equation is consistent for all $i = 1, \ldots, n$, with the clarification exactly the same as in the discussion following Eq. (3.54). Next step is to plug $k = 1$ and $i \to i-1$ in Eq. (3.40) which together with $C_{2-i} = -C_{n+2-i}$ gives

$$(C_i - C_{n+2-i}) |\psi'\rangle = \zeta_{i-1} C_1 |\psi'\rangle \tag{3.57}$$

By adding Eqs. (3.56) and (3.57) and using some elementary trigonometric identities we obtain 3.50. We proceed by fixing $k = (n+1)/2$ and shifting $i \to (n+1)/2 - i$ in Eq. (3.40) to obtain

$$(C_i + C_{n+1-i}) |\psi'\rangle = \zeta_{\frac{n+1}{2}-i} C_{\frac{n+1}{2}} |\psi'\rangle \, , \tag{3.58}$$

satisfied for all $i = 1, \ldots, n$ in the same way as Eq. (3.52). To get Eq. (3.51) and complete the proof to Eq. (3.58) we add

$$(C_i - C_{n+1-i}) |\psi'\rangle = \xi_{i-1} C_{1,-n} |\psi'\rangle \tag{3.59}$$

which is obtained by shifting $i \to i-1$ in Eq. (3.34) □

We are now ready to state and prove our first main result.

Theorem 3. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ be the state and the measurements maximally violating the chained Bell inequality* (2.14). *Then the unitary operation Φ defined above is such that for any pair $i, j = 1, \ldots, n$*

$$\Phi(A'_i B'_j |\psi'\rangle |00\rangle) = |\text{junk}\rangle A_i B_j |\Phi^+\rangle \, , \tag{3.60}$$

$$\Phi(A'_i |\psi'\rangle |00\rangle) = |\text{junk}\rangle A_i |\Phi^+\rangle \, , \qquad \Phi(B'_j |\psi'\rangle |00\rangle) = |\text{junk}\rangle B_j |\Phi^+\rangle \, , \tag{3.61}$$

$$\Phi(|\psi'\rangle |00\rangle) = |\text{junk}\rangle |\Phi^+\rangle \, , \tag{3.62}$$

where $|junk\rangle$ is some irrelevant quantum state, $|\Phi^+\rangle$ is the two-qubit maximally entangled state, and A_i and B_i are given by Eq. (2.15).

Proof. Let us first consider Eq. (3.60). Owing to the linearity of Φ in both Alice's and Bob's measurements and the fact that for even n (see Lemma 2.5):

$$A'_i |\psi'\rangle = \left(s_i X'_A + c_i Z'_A\right) |\psi'\rangle \, , \qquad B'_i |\psi'\rangle = \left(s'_i X'_B + c'_i Z'_B\right) |\psi'\rangle \, , \tag{3.63}$$

the left-hand side of Eq. (3.60) can be rewritten as

$$\begin{aligned} \Phi(A'_i B'_j |\psi'\rangle |00\rangle) \;\; = \;\; & s_i s'_i \Phi(X'_A X'_B |\psi'\rangle |00\rangle) + s_i c'_i \Phi(X'_A Z'_B |\psi'\rangle |00\rangle) \\ & + c_i s'_i \Phi(Z'_A X'_B |\psi'\rangle |00\rangle) + c_i c'_i \Phi(Z'_A Z'_B |\psi'\rangle |00\rangle) . \end{aligned} \tag{3.64}$$

Then, it follows from Eqs. (3.22) and (3.23) that $X_A'X_B'|\psi'\rangle = Z_A'Z_B'|\psi'\rangle = |\psi'\rangle$ and $X_A'Z_B'|\psi'\rangle = -Z_A'X_B'|\psi'\rangle$, and therefore we only need to check how the map Φ applies to $|\psi'\rangle$ and $X_A'Z_B'|\psi'\rangle$. In the first case, one has

$$\begin{aligned}\Phi(|\psi'\rangle|00\rangle) =& \frac{1}{4}\big[(\mathbb{1}+Z_A')(\mathbb{1}+\widetilde{Z}_B)|\psi'\rangle|00\rangle + X_A'(\mathbb{1}-Z_A')(\mathbb{1}+\widetilde{Z}_B)|\psi'\rangle|10\rangle \\ &+ \widetilde{X}_B(\mathbb{1}+Z_A')(\mathbb{1}-\widetilde{Z}_B)|\psi'\rangle|01\rangle + X_A'\widetilde{X}_B(\mathbb{1}-Z_A')(\mathbb{1}-\widetilde{Z}_B)|\psi'\rangle|11\rangle\big].\end{aligned} \tag{3.65}$$

Exploiting Eqs. (3.22) and (3.46) to convert $\widetilde{Z}_B$ to Z_B' and then Z_B' to Z_A', and the fact that Z_A' has eigenvalues ± 1, meaning that $(\mathbb{1}+Z_A')$ and $(\mathbb{1}-Z_A')$ are projectors onto orthogonal subspaces, one finds that the terms in Eq. (3.65) containing the ancillary vectors $|01\rangle$ and $|10\rangle$ simply vanish, and the whole expression simplifies to

$$\Phi(|\psi'\rangle|00\rangle) = \frac{1}{4}\big[(\mathbb{1}+Z_A')^2|\psi'\rangle|00\rangle + X_A'\widetilde{X}_B(\mathbb{1}-Z_A')^2|\psi'\rangle|11\rangle\big]. \tag{3.66}$$

Using then the fact that $(\mathbb{1}\pm Z_A')^2 = 2(\mathbb{1}\pm Z_A')$, the anticommutation relation (3.23) and the identities (3.22) and (3.46), we finally obtain

$$\Phi(|\psi'\rangle|00\rangle) = |\text{junk}\rangle|\Phi^+\rangle \tag{3.67}$$

with $|\text{junk}\rangle = (1/2\sqrt{2})(\mathbb{1}+Z_A')^2|\psi'\rangle$, which is exactly Eq. (3.62).

In the second case, i.e., that of $\Phi(X_A'Z_B'|\psi'\rangle|00\rangle)$, one has

$$\begin{aligned}\Phi(X_A'Z_B'|\psi'\rangle|00\rangle) =& \frac{1}{4}\big[(\mathbb{1}+Z_A')(\mathbb{1}+\widetilde{Z}_B)X_A'Z_B'|\psi'\rangle|00\rangle + X_A'(\mathbb{1}-Z_A')(\mathbb{1}+\widetilde{Z}_B)X_A'Z_B'|\psi'\rangle|10\rangle \\ &+ \widetilde{X}_B(\mathbb{1}+Z_A')(\mathbb{1}-\widetilde{Z}_B)X_A'Z_B'|\psi'\rangle|01\rangle \\ &+ X_A'\widetilde{X}_B(\mathbb{1}-Z_A')(\mathbb{1}-\widetilde{Z}_B)X_A'Z_B'|\psi'\rangle|11\rangle\big].\end{aligned} \tag{3.68}$$

Exploiting the properties (3.22) and (3.46), the anticommutation relation (3.23), and the fact that $(\mathbb{1}+Z_A')(\mathbb{1}-Z_A') = 0$, one can prove that the terms in Eq. (3.68) containing kets $|00\rangle$ and $|11\rangle$ are zero and the whole expression reduces to

$$\Phi(X_A'Z_B'|\psi'\rangle|00\rangle) \;=\; \frac{1}{4}\Big[(\mathbb{1}+Z_A')^2|\psi'\rangle|10\rangle + X_A'Z_A'\widetilde{X}_B(\mathbb{1}-Z_A')^2|\psi'\rangle|01\rangle\Big]. \tag{3.69}$$

By applying then Eq. (3.22) and the anticommutation relation (3.23) in the second term of Eq. (3.69), one can rewrite it as

$$\Phi(X_A'Z_B'|\psi'\rangle|00\rangle) = |\text{junk}\rangle X_A Z_B|\Phi^+\rangle. \tag{3.70}$$

After plugging Eqs. (3.67) and (3.70) into Eq. (3.64) and using the fact that the Pauli matrices X and Z anticommute and satisfy $X_AX_B|\Phi^+\rangle = Z_AZ_B|\Phi^+\rangle = |\Phi^+\rangle$, we arrive at

$$\begin{aligned}\Phi(A_i'B_j'|\psi'\rangle|00\rangle) \;=\;& s_is_i'|\text{junk}\rangle X_AX_B|\Phi^+\rangle + s_ic_i'|\text{junk}\rangle X_AZ_B|\Phi^+\rangle \\ &+ c_is_i'|\text{junk}\rangle Z_AX_B|\Phi^+\rangle + c_ic_i'|\text{junk}\rangle Z_AZ_B|\Phi^+\rangle,\end{aligned} \tag{3.71}$$

which by virtue of the formulas (2.15) is exactly Eq. (3.60).

Let us now prove Eqs. (3.61). From the the linearity of Φ and Eq. (3.63), we get

$$\Phi(A'_i\,|\psi'\rangle\,|00\rangle) = s_i\Phi(X'_A\,|\psi'\rangle\,|00\rangle) + c_i\Phi(Z'_A\,|\psi'\rangle\,|00\rangle).$$

Following the same steps as above, one can prove the following relations

$$\Phi(X'_A\,|\psi'\rangle\,|00\rangle) = |\mathrm{junk}\rangle\,X_A\,|\Phi^+\rangle\,, \qquad \Phi(Z'_A\,|\psi'\rangle\,|00\rangle) = |\mathrm{junk}\rangle\,Z_A\,|\Phi^+\rangle\,,$$

which when plugged into Eq. (3.72) leads, in virtue of Eq. (3.63), to the first part of Eq. (3.61).The second part of the same equation can be proven in exactly the same way. □

Let us notice that in order to prove the uniqueness of correlations maximally violating the chained Bell inequality one needs only the conditions (3.61) and (3.62); the conditions (3.60) are superfluous. This is because

$$\begin{aligned}\langle\psi'|A'_i\otimes B'_j|\psi'\rangle &= (\langle 00|\langle\psi'|A'_i)\Phi^\dagger\Phi(B'_j\,|\psi'\rangle\,|00\rangle)\\ &= \langle\Phi^+|A_i\otimes B_j|\Phi^+\rangle,\end{aligned}$$

where the first equality follows from the fact that Φ is unitary and and second from Eqs. (3.61) and (3.62).

3.3 Robustness

For practical purposes, it is important to estimate the robustness of self-testing procedures, as in any realistic situation it is impossible due to experimental imperfections to actually reach the maximal violation of any Bell inequality. One expects, however, self-testing procedures to tolerate some deviations from the ideal case, that is, if the violation of the given Bell inequality is close to its maximum quantum value, the state producing the violation must be close to the state maximally violating this Bell inequality. In [YN13] it has been proven that SOS decompositions allow to reach good robustness of all analytical self-test protocols.

Here we study how robust is the above self-testing procedure based on the chained Bell inequality. Assuming that the physical state $|\psi'\rangle$ and the physical measurements A'_i and B'_i violate the chained Bell inequality by $\beta^n_Q - \varepsilon$ with some sufficiently small $\varepsilon > 0$, we estimate the distance between $|\psi'\rangle$ and the reference state, and how this distance is affected when physical measurements are applied to it.

Let us begin by noticing that now $\langle\psi'|(\beta^n_Q\mathbb{1} - \mathscr{B}^n_{ch})|\psi'\rangle = \varepsilon$, and therefore the exact relations (3.76), (3.77) and (3.92) do not hold anymore. We then need to derive their approximate versions. First, let us state and prove the following Lemma, stemming from the first SOS decomposition.

Lemma 3.1. *Let $|\psi'\rangle$ and $\{A'_i, B'_i\}$ be the state and the measurements violating the chained Bell inequality by $\beta_Q^n - \varepsilon$. Then, the following relations are satisfied:*

$$\|(A'_i - B'_{i-1,i})\,|\psi'\rangle\,\| \le \sqrt{\frac{\varepsilon}{\cos(\pi/2n)}} \equiv \sqrt{\varepsilon_1} \tag{3.72}$$

for $i = 1, \ldots, n$,

$$\|(\alpha_i B'_j + \beta_i B'_{i+j} + \gamma_i B'_{i+j+1})\,|\psi'\rangle\,\| \le \sqrt{\varepsilon_1} \tag{3.73}$$

for $i = 1, \ldots, n-2$ and $j = 1, \ldots, n$, and

$$\|(A'_i \otimes B'_i - A'_{i+1} \otimes B'_{i+1})\,|\psi'\rangle\,\| \le \sqrt{8n\cos\frac{\pi}{2n}\varepsilon} \equiv \sqrt{n\varepsilon_2}, \tag{3.74}$$

$$\|(A'_i \otimes B'_{i-1} - A'_{i+1} \otimes B'_i)\,|\psi'\rangle\,\| \le \sqrt{n\varepsilon_2} \tag{3.75}$$

for $i = 1, \ldots, n$.

Proof. All equations follow directly from SOS decompositions. When a chained Bell inequality is violated by $2n\cos[\pi/2n] - \varepsilon$, from the definition of SOS decomposition it follows that $\sum_i \langle\psi'|P_i^2|\psi'\rangle = \varepsilon$ and consequently $||P_i|\psi'\rangle|| \le \sqrt{\varepsilon}$ for all i. The expressions given by equations (3.72) and (3.73) are identified in the first degree SOS decomposition (3.1) (note the explanation after the equation), while the expressions bounded in equations (3.74) and (3.75) are the part of the second degree SOS decomposition (3.17). □

Taking into account definitions of operators X'_A, X'_B, Z'_A and Z'_B given in Eqs. 3.19 and 3.20, Lemma 3.1 implies:

$$\|(X'_A - X'_B)\,|\psi'\rangle\,\| \le \sqrt{\varepsilon_1(n)}, \qquad \|(Z'_A - Z'_B)\,|\psi'\rangle\,\| \le \sqrt{\varepsilon_1(n)}, \tag{3.76}$$

where $\varepsilon_1 = \varepsilon/\cos(\pi/2n)$. Clearly, for any n, $\varepsilon_1(n) \le \sqrt{2}$ and $\varepsilon_1(n) \to 0$ for $\varepsilon \to 0$. Moreover, following the same reasoning as in (3.47), one proves that

$$\|(\widetilde{X}'_B - X'_B)\,|\psi'\rangle\,\| \le \sqrt{\varepsilon_1(n)}, \qquad \|(\widetilde{Z}'_B - Z'_B)\,|\psi'\rangle\,\| \le \sqrt{\varepsilon_1(n)}. \tag{3.77}$$

Finally, both SOS decompositions (3.1) and (3.17) imply the following approximate anticommutation relations given in the following Lemma:

Lemma 3.2. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ be the state and the measurements violating the chained Bell inequality by $\beta_Q^n - \varepsilon$. Then, the following approximate anticommutation relations are true*

$$\|\{A'_1, A'_{\frac{n}{2}+1}\}\,|\psi'\rangle\,\| \le \sqrt{2\varepsilon_1} + \frac{1}{\xi_{n/2-1}}\left(\frac{4\sqrt{\varepsilon_1}}{\alpha_{n/2-1}} + n\sqrt{2\varepsilon_2}\right) = \omega_{\text{ev}} \tag{3.78}$$

for even n, and

$$\begin{aligned}\|\{A'_1, A'_{\frac{n+1}{2}} + A'_{\frac{n+3}{2}}\}\,|\psi'\rangle\,\| &\leq 2\sqrt{\varepsilon_1 n}\left(\frac{\sqrt{2}}{\zeta_{(n-1)/2}} + \sqrt{n-1}\right) + \sqrt{\varepsilon_1}(1+\sqrt{2}) \\ &\quad + \frac{3\sqrt{\varepsilon_1}}{\cos\frac{\pi}{2n}\alpha_{(n-1)/2}\zeta_{(n-1)/2}}\left(2 + \frac{\gamma_{(n-1)/2}}{\alpha_1}\right) = \omega_{\mathrm{odd}}\end{aligned} \tag{3.79}$$

for odd n. For any fixed n the right-hand sides of both inequalities vanish if $\varepsilon \to 0$ *and for sufficiently large n both functions scale quadratically with n.*

Proof. The proof goes along the same lines as that of Lemma 2.4, however, at each step we need to take into account the error stemming from the fact that now the Bell inequality is not violated maximally. We prove the cases of even and odd n separately.

Even number of measurements. We first need to prove the approximate versions of the identities (3.33) and (3.34). By substituting $j = k - i$ in (3.73) we obtain

$$\|(\alpha_i C_{k-i} + \beta_i C_k + \gamma_i C_{k+1})\,|\psi'\rangle\,\| \leq \sqrt{\varepsilon_1} \tag{3.80}$$

Then, by shifting $i \to n - i - 1$ and setting $j = k + i + 1$ in (3.73), we have

$$\|(\alpha_i C_{k+i+1} + \gamma_i C_k + \beta_i C_{k+1})\,|\psi'\rangle\,\| \leq \sqrt{\varepsilon_1}. \tag{3.81}$$

Both inequalities imply

$$\|(C_{k-i} + C_{k+i+1} - \xi_i C_{k,k+1})\,|\psi'\rangle\,\| \leq \frac{2\sqrt{\varepsilon_1}}{\alpha_i} \tag{3.82}$$

for any $k = 1, \ldots, n$ and $i = 1, \ldots, n-2$. The case when $i = n-1$ or $i = n$ are trivial because they represent the definition of $C_{k,k+1}$. Then, by using Eq. (3.80) with $k = n$ and Eq. (3.81) with $k = 0$, one can prove the following inequality

$$\|(C_{i+1} - C_{n-i} - \xi_i C_{1,-n})\,|\psi'\rangle\,\| \leq \frac{2\sqrt{\varepsilon_1}}{\alpha_i} \tag{3.83}$$

with $i = 1, \ldots, n-2$. Now, one has

$$\begin{aligned}\|\{A'_1, A'_{\frac{n}{2}+1}\}\,|\psi'\rangle\,\| &= \|(A'_1 A'_{\frac{n}{2}+1} + A'_{\frac{n}{2}+1} A'_1)\,|\psi'\rangle\,\| \\ &\leq \|(A'_1 B'_{\frac{n}{2},\frac{n}{2}+1} + A'_{\frac{n}{2}+1} B'_{1,-n})\,|\psi'\rangle\,\| + \sqrt{2\varepsilon_1},\end{aligned}$$

which with the aid of Eq. (3.82) with $k = n/2$ and $i = n/2 - 1$ and Eq. (3.83) with $i = n/2 - 1$, can be further upper bounded as

$$\begin{aligned}\left\|\{A'_1, A'_{\frac{n}{2}+1}\}\,|\psi'\rangle\right\| &\leq \frac{1}{\xi_{n/2-1}}\left\|\left[A'_1(B'_1 + B'_n) + A'_{\frac{n}{2}+1}(B'_{\frac{n}{2}} - B'_{\frac{n}{2}+1})\right]|\psi'\rangle\right\| + \frac{1}{\xi_{n/2-1}}\frac{4\sqrt{\varepsilon_1}}{\alpha_{n/2-1}} \\ &\leq \frac{1}{\xi_{n/2-1}}\left[\left\|(A'_1 B'_1 - A'_{\frac{n}{2}+1} B'_{\frac{n}{2}+1})\,|\psi'\rangle\right\| + \left\|(A'_1 B'_n + A'_{\frac{n}{2}+1} B'_{\frac{n}{2}})\,|\psi'\rangle\right\|\right] \\ &\quad + \frac{1}{\xi_{n/2-1}}\frac{4\sqrt{\varepsilon_1}}{\alpha_{n/2-1}}.\end{aligned} \tag{3.84}$$

To upper bound the above two terms, we will use approximate versions of Eqs. (3.36) and (3.37). First, it follows from the SOS decomposition that for any $j = 1, \dots, n$:

$$\sum_{i=1}^{j} \left\| (A'_i B'_i - A'_{i+1} B'_{i+1}) \, |\psi'\rangle \right\|^2 \leq n\varepsilon_2, \tag{3.85}$$

which by virtue of the triangle inequality for the norm and concavity of the square root implies

$$\begin{aligned} \left\| (A'_1 B'_1 - A'_{j+1} B'_{j+1}) \, |\psi'\rangle \right\| &= \left\| \sum_{i=1}^{j} (A'_i B'_i - A'_{i+1} B'_{i+1}) \, |\psi'\rangle \right\| \\ &\leq \sum_{i=1}^{j} \left\| (A'_i B'_i - A'_{i+1} B'_{i+1}) \, |\psi'\rangle \right\| \\ &\leq \sqrt{j} \left(\sum_{i=1}^{j} \left\| (A'_i B'_i - A'_{i+1} B'_{i+1}) \, |\psi'\rangle \right\|^2 \right)^{\frac{1}{2}} \\ &\leq \sqrt{jn\varepsilon_2}. \end{aligned} \tag{3.86}$$

Analogously, the SOS decomposition (3.17) implies that

$$\sum_{i=1}^{j} \left\| (A'_i B'_{i-1} - A'_{i+1} B'_i) \, |\psi'\rangle \right\|^2 \leq \sqrt{n\varepsilon_2}, \tag{3.87}$$

from which, by using similar arguments as above, one infers that

$$\left\| (A'_1 B'_n + A'_{j+1} B'_j) \, |\psi'\rangle \right\| = \sum_{i=1}^{j} \left\| (A'_i B'_{i-1} - A'_{i+1} B'_i) \, |\psi'\rangle \right\| \leq \sqrt{jn\varepsilon_2}. \tag{3.88}$$

Substituting $j = n/2$ and applying both inequalities (3.86) and (3.88) to (3.84) one finally obtains (3.78).

Odd number of measurements. We first prove the following inequality

$$\| (C_{k-i} + C_{k+i} - \zeta_i C_k) \, |\psi'\rangle \| \leq \left(2 + \frac{\gamma_i}{\alpha_1} \right) \frac{\sqrt{\varepsilon_1}}{\alpha_i} \tag{3.89}$$

for any $i = 1, \dots, n-2$. Then, from inequalities (3.86) and (3.88) with $j = (n-1)/2$, and inequality (3.89) for $i = (n-1)/2$ and $k = n$, one obtains

$$\left\| \left[A'_1 (B'_1 + B'_n) - \zeta_{\frac{n-1}{2}} A'_{\frac{n+1}{2}} B'_n \right] |\psi'\rangle \right\| \quad \leq \quad \sqrt{2n(n-1)\varepsilon_2} + \varepsilon',$$

where we denoted

$$\varepsilon' = \frac{\sqrt{\varepsilon_1}}{\alpha_{(n-1)/2}} \left(2 + \frac{\gamma_{(n-1)/2}}{\alpha_1} \right).$$

Analogously, from inequalities (3.86) and (3.88) with $j=(n+1)/2$ and inequality (3.89) for $i=(n-1)/2$ and $k=n+1$, one obtains

$$\left\|\left[A'_1(B'_1+B'_n)+\zeta_{\frac{n-1}{2}}A'_{\frac{n+3}{2}}B'_n\right]|\psi'\rangle\right\| \;\leq\; \sqrt{2n(n-1)\varepsilon_2}+\varepsilon'. \tag{3.90}$$

We can then upper bound

$$\begin{aligned}
\left\|\{A'_1,A'_{\frac{n+1}{2}}+A'_{\frac{n+3}{2}}\}\,|\psi'\rangle\right\| \;\leq\;& \frac{1}{2\cos(\frac{\pi}{2n})}\left\|[A'_1(B'_{\frac{n-1}{2}}+2B'_{\frac{n+1}{2}}+B'_{\frac{n+3}{2}})\right.\\
&\left.+(A'_{\frac{n+1}{2}}+A'_{\frac{n+3}{2}})(B'_1-B'_n)]\,|\psi'\rangle\right\|+\sqrt{\varepsilon_1}(1+\sqrt{2})\\
\leq{}& \frac{1}{2\cos(\frac{\pi}{2n})}\left\|\left[A'_1\left(B'_{\frac{n-1}{2}}+B'_{\frac{n+3}{2}}+2\frac{B'_1+B'_n}{\zeta_{(n-1)/2}}\right)+(A'_{\frac{n+1}{2}}+A'_{\frac{n+3}{2}})(B'_1-B'_n)\right]|\psi'\rangle\right\|\\
&+\sqrt{\varepsilon_1}(1+\sqrt{2})+\frac{\varepsilon'}{2\cos(\pi/2n)\zeta_{(n-1)/2}}\\
\leq{}& \frac{1}{2\cos(\frac{\pi}{2n})}\left\|\left(A'_1B'_{\frac{n-1}{2}}+A'_1B'_{\frac{n+3}{2}}+A'_{\frac{n+1}{2}}B'_1-A'_{\frac{n+3}{2}}B'_n\right)|\psi'\rangle\right\|\\
&+\sqrt{\varepsilon_1}(1+\sqrt{2})+\frac{3\varepsilon'}{2\cos(\pi/2n)\zeta_{(n-1)/2}}+2\sqrt{\varepsilon_1 n(n-1)}.
\end{aligned} \tag{3.91}$$

In the first inequality we used (3.72) twice in parallel (to exchange A'_{n+2} and A'_{n+3} with corresponding B's) and once more separately (to exchange A'_1 with $B'_{1,-n}$). To get the second inequality we used (3.89) and for the final inequality we used twice (3.90). Inequality (3.89) for $k=1$ and $i=(n-1)/2$ gives

$$\left\|[A'_{\frac{n+1}{2}}-A'_{\frac{n+3}{2}}-\zeta_{\frac{n-1}{2}}A'_1]\,|\psi'\rangle\right\|\leq\varepsilon',$$
$$\left\|[B'_{\frac{n+1}{2}}-B'_{\frac{n+3}{2}}-\zeta_{\frac{n-1}{2}}B'_1]\,|\psi'\rangle\right\|\leq\varepsilon'$$

with $C=A,B$, while for $k=n$ and $i=(n-1)/2$

$$\left\|[B'_{\frac{n+1}{2}}-B'_{\frac{n-1}{2}}-\zeta_{\frac{n-1}{2}}B'_n]\,|\psi'\rangle\right\|\leq\varepsilon',$$

These three inequalities when applied to (3.91) give

$$\begin{aligned}
\left\|\{A'_1,A'_{\frac{n+1}{2}}+A'_{\frac{n+3}{2}}\}\,|\psi'\rangle\right\| \;\leq\;& \frac{1}{2\cos(\frac{\pi}{2n})\zeta_{\frac{n-1}{2}}}\left\|\left(A'_{\frac{n+1}{2}}B'_{\frac{n-1}{2}}-A'_{\frac{n+3}{2}}B'_{\frac{n+1}{2}}\right.\right.\\
&\left.\left.+A'_{\frac{n+1}{2}}B'_{\frac{n+1}{2}}-A'_{\frac{n+3}{2}}B'_{\frac{n+3}{2}}\right)|\psi'\rangle\right\|\\
&+\sqrt{\varepsilon_1}(1+\sqrt{2})+\frac{3\varepsilon'}{\cos\frac{\pi}{2n}\zeta_{(n-1)/2}}+2\sqrt{\varepsilon_1 n(n-1)}.
\end{aligned}$$

To upper bound the norm appearing on the right-hand side and complete the proof we use inequalities (3.74) and (3.75) with $i = (n+1)/2$ which leads us to

$$\begin{aligned}\left\|\{A'_1, A'_{\frac{n+1}{2}} + A'_{\frac{n+3}{2}}\}\,|\psi'\rangle\right\| \;\leq\; & 2\sqrt{\varepsilon_1 n}\left(\frac{\sqrt{2}}{\zeta_{(n-1)/2}} + \sqrt{n-1}\right) + \sqrt{\varepsilon_1}(1+\sqrt{2}) \\ & + \frac{3\sqrt{\varepsilon_1}}{\cos\frac{\pi}{2n}\alpha_{(n-1)/2}\zeta_{(n-1)/2}}\left(2 + \frac{\gamma_{(n-1)/2}}{\alpha_1}\right).\end{aligned}$$

To complete the proof let us notice that both ω_{ev} and ω_{odd}, defined in Eqs. (3.78) and (3.79) respectively, vanish when $\varepsilon \to 0$. Furthermore, the term dominating the scaling of ω_{ev} with n for large n is $4\varepsilon_1/(\xi_{n/2-1}\alpha_{n/2-1}) = 2\sqrt{\varepsilon}/(\sin^2(\pi/2n))$. It follows that for sufficiently large n the function $1/\sin^2(\pi/2n)$ behaves like $(4/\pi^2)n^2 + 1/3 + O(1/n^2)$ and therefore we can conclude that ω_{ev} scales quadratically with n when n is large enough, and for small ε it behaves as $\sqrt{\varepsilon}$. After analogous analysis one finds that ω_{odd} exhibits the same behaviour for small ε and sufficiently large n. □

Having the results of Lemma 3.2 we can infer that for the operators used in the isometry the following robust anticommutation inequality holds (in case of even n)

$$\|\{X'_A, Z'_A\}\,|\psi'\rangle\,\| \leq \sqrt{2\varepsilon_1(n)} + \frac{1}{\xi_{n/2-1}}\left(\frac{4\sqrt{\varepsilon_1(n)}}{\alpha_{n/2-1}} + n\sqrt{2\varepsilon_2(n)}\right) = \omega_{\mathrm{ev}}(n), \qquad (3.92)$$

where $\xi_i = 2\cos(2i+1)\pi/2n$, α_i is defined in Lemma 2.1, and ε_1 and ε_2 are given in Lemma 3.2. Analogous statement holds when n is odd. In what follows we drop the dependence of ε_1 and ε_2 on n.

Before stating the main theorem about the robustness of our self-test we have to state and prove two more lemmas. The first one Lemma 3.3 will be useful for the robustness of measurements self-testing. The second one, Lemma 3.4, takes into account the missnormalization of the $|\text{junk}\rangle$ following from the non-maximal violation of the corresponding chained Bell inequality.

Lemma 3.3. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ be a state and measurements violating the chained Bell inequalities by $\beta_Q^n - \varepsilon$. Then, for an even number of measurements:*

$$\left\|\left(A'_i - s_i A'_{\frac{n}{2}+1} - c_i A'_1\right)|\psi'\rangle\right\| \leq g_{\mathrm{ev}}(\varepsilon, n),$$
$$\left\|\left(B'_i - s'_i B'_{\frac{n}{2},\frac{n}{2}+1} - c'_i B'_{1,-n}\right)|\psi'\rangle\right\| \leq h_{\mathrm{ev}}(\varepsilon, n),$$

while for an odd number of measurements:

$$\left\|\left(A'_i - s_i A'_{\frac{n+1}{2},\frac{n+3}{2}} - c_i A'_1\right)|\psi'\rangle\right\| \leq g_{\mathrm{odd}}(\varepsilon, n),$$
$$\left\|\left(B'_i - s'_i B'_{\frac{n+1}{2}} - c'_i B'_{1,-n}\right)|\psi'\rangle\right\| \leq h_{\mathrm{odd}}(\varepsilon, n).$$

The functions g_{ev}, h_{ev}, g_{odd} and h_{odd} vanish for $\varepsilon \to 0$ and scale linearly with n.

Proof. We will follow the proof of Lemma 2.5. We can write

$$\begin{aligned}
&\left\| \left(A'_i - s_i A'_{\frac{n}{2}+1} - c_i A'_1 \right) |\psi'\rangle \right\| \\
&= \tfrac{1}{2} \left\| \left(A'_i - A'_{2-i} - \zeta_{\frac{n}{2}+1-i} A'_{\frac{n}{2}+1} + A'_i + A'_{2-i} - \zeta_{i-1} A'_1 \right) |\psi'\rangle \right\| \\
&\leq \tfrac{1}{2} \left\| \left(A'_i - A'_{2-i} - \zeta_{\frac{n}{2}+1-i} A'_{\frac{n}{2}+1} \right) |\psi'\rangle \right\| + \tfrac{1}{2} \left\| \left(A'_i + A'_{2-i} - \zeta_{i-1} A'_1 \right) |\psi'\rangle \right\| \\
&\leq \left(1 + \tfrac{\gamma_{|\frac{n}{2}+1-i|}}{2\alpha_1} \right) \tfrac{\sqrt{\varepsilon_1}}{\alpha_{|\frac{n}{2}+1-i|}} + \left(1 + \tfrac{\gamma_{i-1}}{2\alpha_1} \right) \tfrac{\sqrt{\varepsilon_1}}{\alpha_{i-1}} = g_{\text{ev}}
\end{aligned} \tag{3.93}$$

The equality corresponds to the pair of Eqs. (3.52) and (3.53), while the first inequality is the triangle inequality followed by the bounds from Eq. (3.89). The absolute value appearing in $\gamma_{|\frac{n}{2}+1-i|}$ and $\alpha_{|\frac{n}{2}+1-i|}$ is justified in the discussion after Eq. (3.52). Note that this bound cannot be applied to the cases when $i = 1, n/2+1, n$ because for these cases coefficients α_i and γ_i are not defined. The cases $i = 1, n/2+1$ are trivial statements and $g_{\text{ev}} = 0$, while for the case $i = n$ the norm $\left\| \left(A'_i + A'_{2-i} - \zeta_{i-1} A'_1 \right) |\psi'\rangle \right\| \leq \sqrt{\varepsilon_1/\alpha_1}$ is obtained by fixing $j = n$ and $i = 1$ in (3.73), so $g_{\text{ev}} = (1 + \gamma_{|\frac{n}{2}+1-i|}/2\alpha_1)(\sqrt{\varepsilon_1}/\alpha_{|\frac{n}{2}+1-i|}) + \sqrt{\varepsilon_1/\alpha_1}/2$. Similarly it can be shown that:

$$\begin{aligned}
&\left\| \left(B'_i - s'_i B'_{\frac{n}{2},\frac{n}{2}+1} - c'_i B'_{1,-n} \right) |\psi'\rangle \right\| \\
&= \tfrac{1}{2} \left\| \left(B'_i - B'_{1-i} - \xi_{\frac{n}{2}-i} B'_{\frac{n}{2},\frac{n}{2}+1} + B'_i + B'_{1-i} - \xi_{i-1} B'_{1,-n} \right) |\psi'\rangle \right\| \\
&\leq \tfrac{1}{2} \left\| \left(B'_i - B'_{1-i} - \xi_{\frac{n}{2}-i} B'_{\frac{n}{2},\frac{n}{2}+1} \right) |\psi'\rangle \right\| + \tfrac{1}{2} \left\| \left(B'_i + B'_{1-i} - \xi_{i-1} B'_{1,-n} \right) |\psi'\rangle \right\| \\
&\leq \sqrt{\varepsilon_1} \left(\tfrac{1}{\alpha_{i-1}} + \tfrac{1}{\tilde{\alpha}_{\frac{n}{2}-i}} \right) = h_{\text{ev}},
\end{aligned} \tag{3.94}$$

where in the last inequality we used already established bounds given in Eqs. (3.82) and (3.83) and we introduced notation $\tilde{\alpha}_{n/2-i}$ which is equal to $\alpha_{n/2-i}$ when $n/2 > i$, and to $\alpha_{i-1-n/2}$ otherwise (for the clarification see the text following Eq. (3.54)). Similarly to the previous case the bound is properly defined unless $i \in \{1, n, n/2, n/2+1\}$. For the cases $i = 1, n$ the norm $\| (B'_i + B'_{1-i} - \xi_{i-1} B'_{1,-n}) |\psi'\rangle \|$ is trivial, thus equal to 0, so we have $h_{\text{ev}} = \sqrt{\varepsilon_1}/\tilde{\alpha}_{n/2-i}$. Analogously, when $i = n/2, n/2+1$, the norm $\| (B'_i - B'_{1-i} - \xi_{\frac{n}{2}-i} B'_{\frac{n}{2},\frac{n}{2}+1}) |\psi'\rangle \|$ is equal to 0, causing h_{ev} to be equal to $\sqrt{\varepsilon_1}/\alpha_{i-1}$. By repeating analogue procedure it is easy to obtain bounds for the case when the number of inputs is odd:

$$\begin{aligned}
g_{\text{odd}} &= \sqrt{\varepsilon_1} \left(\tfrac{1}{\tilde{\alpha}_{\frac{n+1}{2}-i}} + \left(1 + \tfrac{\gamma_{i-1}}{2\alpha_1} \right) \tfrac{1}{\alpha_{i-1}} \right), \\
h_{\text{odd}} &= \sqrt{\varepsilon_1} \left(\tfrac{1}{\alpha_{i-1}} + \left(1 + \tfrac{\gamma_{|\frac{n+1}{2}-i|}}{2\alpha_1} \right) \tfrac{1}{\alpha_{|\frac{n+1}{2}-i|}} \right).
\end{aligned}$$

Similarly to the case when the number of inputs is even for $i = 1, n$ the expression for g_{odd} is estimated to be $\sqrt{\varepsilon_1}/\tilde{\alpha}_{\frac{n+1}{2}-i}$ and for $i = (n+1)/2, (n+3)/2$ it reduces to

$[\sqrt{\varepsilon_1}/\alpha_{i-1}]\,(1+\gamma_{i-1}/(2\alpha_1))$. Also, for $i=(n+1)/2$ we have $h_{\mathrm{odd}}=\sqrt{\varepsilon_1}/\alpha_{i-1}$,and for $i=1,n$ we estimate $h_{\mathrm{odd}}=[\sqrt{\varepsilon_1}/\alpha_{|\frac{n+1}{2}-i|}](1+\gamma_{|\frac{n+1}{2}-i|}/(2\alpha_1))$.

In the worst case functions g_{ev},h_{ev},g_{odd} and h_{odd} behave as $\sin^{-1}(\pi/n)$ when n is sufficiently large. Linear scaling with respect to n of the aforementioned functions when n is sufficiently large can be confirmed by considering the behaviour of function $\sin^{-1}(\pi/n)$ when n is large enough. □

Lemma 3.4. *Let* $|\mathrm{junk}\rangle$ *be the state of the additional degrees of freedom from Theorem 3 and* $|\mathrm{junk}'\rangle$ *state defined in Eq. (3.106). Then,*

$$\|\,|\mathrm{junk}\rangle-|\mathrm{junk}'\rangle\,\|\leq\left(\frac{1}{2}+\sqrt{2}\right)\sqrt{\varepsilon_1}+\frac{\omega'}{4}, \tag{3.95}$$

where $\omega'\equiv\omega_{\mathrm{ev}}$ *for even n and* $\omega'\equiv\omega_{\mathrm{odd}}$ *for odd n.*

Proof. Let us notice that $\|\,|\mathrm{junk}\rangle-|\mathrm{junk}'\rangle\,\|=\|\,|\mathrm{junk}'\rangle\,\|-1$ and then by using the explicit form of $|\mathrm{junk}'\rangle$ and the inequalities (3.76) and (3.77), we can write

$$\begin{aligned}\|\,|\mathrm{junk}'\rangle\,\| &\leq \frac{1}{2\sqrt{2}}\left(\|(\mathbb{1}+Z_A')(\mathbb{1}+Z_B')\,|\psi'\rangle\,\|+2\sqrt{\varepsilon_1}\right)\\ &\leq \frac{1}{2\sqrt{2}}\left[\|(\mathbb{1}+Z_A')^2\,|\psi'\rangle\,\|+4\sqrt{\varepsilon_1}\right]\\ &= \frac{1}{\sqrt{2}}\|(\mathbb{1}+Z_A')\,|\psi'\rangle\,\|+\sqrt{2\varepsilon_1}\end{aligned} \tag{3.96}$$

Now we want to estimate $|\,\langle\psi'|Z_A'\,|\psi'\rangle\,|$. For this we will follow a similar estimation presented in [MYS14]. Note that due to the unitarity of Z_A', and Eqs. (3.76) and (3.92) we can write $\|\,(Z_A'X_B'+X_A'Z_A')\,|\psi'\rangle\,\|\;=\|\,(Z_A'X_B'-Z_A'X_A'+Z_A'X_A'+X_A'Z_A')\,|\psi'\rangle\,\|\;\leq\sqrt{\varepsilon_1}+\omega'$. The norm will not change if we multiply the expression in brackets by some unitary operator. This means that $|\,\langle\psi'|Z_A'\,|\psi'\rangle+\langle\psi'|X_B'X_A'Z_A'\,|\psi'\rangle\,|\leq\sqrt{\varepsilon_1}+\omega'$. We can put the same bound for the complex conjugated expression

$$|\,\langle\psi'|Z_A'\,|\psi'\rangle+\langle\psi'|X_B'Z_A'X_A'\,|\psi'\rangle\,|\leq\sqrt{\varepsilon_1}+\omega'. \tag{3.97}$$

On the other hand, using unitarity of Z_A' and result (3.76) we can write

$$|\,\langle\psi'|Z_A'\,|\psi'\rangle-\langle\psi'|X_B'Z_A'X_A'\,|\psi'\rangle\,|\leq\sqrt{\varepsilon_1}. \tag{3.98}$$

Finally if we sum Eqs. (3.97) and (3.98) we get

$$|\,\langle\psi'|Z_A'\,|\psi'\rangle\,|\leq\sqrt{\varepsilon_1}+\omega'/2 \tag{3.99}$$

If we plug this result in (3.96) we will get

$$\begin{aligned}\|\;|\mathrm{junk}'\rangle\,\| &\leq\sqrt{\langle\psi'|\,(\mathbb{1}+Z_A')\,|\psi'\rangle}+\sqrt{2\varepsilon_1}\\ &\leq\sqrt{1+\sqrt{\varepsilon_1}+\omega'/2}+\sqrt{2\varepsilon_1}\\ &\leq 1+(\tfrac{1}{2}+\sqrt{2})\sqrt{\varepsilon_1}+\tfrac{\omega'}{4}\end{aligned} \tag{3.100}$$

This estimation concludes the proof, since it is easy to check that the Eq. (3.95) is satisfied. □

Equipped with these tools we can state and prove the second main result of this chapter.

Theorem 4. *Let $\{|\psi'\rangle, A_i', B_i'\}$ be a state and measurements giving violation of the chained Bell inequality $\beta_Q^n - \varepsilon$. Then,*

$$\|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - |\text{junk}\rangle A_iB_j|\Phi^+\rangle\| \leq f_{ij}(\varepsilon,n), \tag{3.101}$$

$$\|\Phi(A_i'|\psi'\rangle|00\rangle) - |\text{junk}\rangle A_i|\Phi^+\rangle\| \leq f_{A_i}(\varepsilon,n), \tag{3.102}$$

$$\|\Phi(B_j'|\psi'\rangle|00\rangle) - |\text{junk}\rangle B_j|\Phi^+\rangle\| \leq f_{B_j}(\varepsilon,n), \tag{3.103}$$

$$\|\Phi(|\psi'\rangle|00\rangle) - |\text{junk}\rangle|\Phi^+\rangle\| \leq f(\varepsilon,n), \tag{3.104}$$

where $i,j = 1,\ldots,n$, Φ is the unitary transformation defined above, $|\text{junk}\rangle = (1/N)(\mathbb{1} + Z_A')(\mathbb{1} + \widetilde{Z}_B')|\psi'\rangle$ with N denoting the length of $|\text{junk}\rangle$. The functions $f(\varepsilon,n)$, $f_{B_j}(\varepsilon,n)$, $f_{A_i}(\varepsilon,n)$ and $f_{ij}(\varepsilon,n)$ vanish as $\varepsilon \to 0$ and for sufficiently large n scale with n as n^2.

Proof. As the norm N of $|\text{junk}\rangle$ cannot be computed exactly, it turns out that to prove this theorem it is more convenient to first estimate the following distance

$$\|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - |\text{junk}'\rangle A_iB_j|\Phi^+\rangle\| \tag{3.105}$$

with

$$|\text{junk}'\rangle = \frac{1}{2\sqrt{2}}(\mathbb{1} + Z_A')(\mathbb{1} + \widetilde{Z}_B')|\psi'\rangle. \tag{3.106}$$

and then show that the error we have by doing so is small for sufficiently small ε.

From now on we will mainly follow the steps of the proof of Theorem 3 replacing the identities by the corresponding inequalities. First, let us notice that for any $i = 1,\ldots,n$:

$$\|[A_i' - (s_iX_A' + c_iZ_A')]|\psi'\rangle\| \leq g_{\text{ev}}, \qquad \|[B_i' - (s_i'X_B' + c_i'Z_B')]|\psi'\rangle\| \leq h_{\text{ev}}. \tag{3.107}$$

where g_{ev} and h_{ev} are given in Lemma 3.3. Denoting by $\overline{A}_i$ and $\overline{B}_i$ the operators appearing in the parentheses in (3.107), we can write

$$\begin{aligned} &\|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - |\text{junk}'\rangle A_iB_j|\Phi^+\rangle\| \leq \\ &\leq \|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - \Phi(\overline{A}_i\overline{B}_j|\psi'\rangle|00\rangle)\| + \|\Phi(\overline{A}_i\overline{B}_j|\psi'\rangle|00\rangle) - |\text{junk}'\rangle A_iB_j|\Phi^+\rangle\|, \end{aligned} \tag{3.108}$$

and, by further exploitation of the fact that Φ is unitary, the first norm can be upper bounded as

$$\begin{aligned} \|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - \Phi(\overline{A}_i\overline{B}_j|\psi'\rangle|00\rangle)\| &\leq \|(A_i'B_j' - \overline{A}_i\overline{B}_j)|\psi'\rangle\| \\ &\leq \|(A_i' - \overline{A}_i)|\psi'\rangle\| + \|(B_j' - \overline{B}_j)|\psi'\rangle\| \\ &\leq g_{\text{ev}} + h_{\text{ev}}, \end{aligned} \tag{3.109}$$

where to obtain the second inequality we have used the standard trick of adding and subtracting the term $A'_i\overline{B}_j\,|\psi'\rangle$, the triangle inequality for the norm, and the fact that A_i is unitary and that the spectral radius of $\overline{B}_j$ is not larger than one. The third inequality in (3.109) stems directly from (3.107). In the cases when A'_i or B'_j are equal to the identity operator $\mathbb{1}$, the above bound is replaced by h_{ev} and g_{ev}, respectively, while in the case $A'_i = B'_j = \mathbb{1}$, this distance is simply zero.

Let us then concentrate on the second norm on the right-hand side of (3.108). Exploiting the explicit forms of the operators $\overline{A}_i$ and $\overline{B}_i$ and the measurements A_i and B_i, one has

$$\begin{aligned}\|\Phi(\overline{A}_i\overline{B}_j\,|\psi'\rangle\,|00\rangle) - |\mathrm{junk}'\rangle\,A_iB_j\,|\Phi^+\rangle\,\| \leq\; & \|\Phi(X'_AX'_B\,|\psi'\rangle\,|00\rangle) - |\mathrm{junk}'\rangle\,X_AX_B\,|\Phi^+\rangle\,\| \\ & + \|\Phi(X'_AZ'_B\,|\psi'\rangle\,|00\rangle) - |\mathrm{junk}'\rangle\,X_AZ_B\,|\Phi^+\rangle\,\| \\ & + \|\Phi(Z'_AX'_B\,|\psi'\rangle\,|00\rangle) - |\mathrm{junk}'\rangle\,Z_AX_B\,|\Phi^+\rangle\,\| \\ & + \|\Phi(Z'_AZ'_B\,|\psi'\rangle\,|00\rangle) - |\mathrm{junk}'\rangle\,Z_AZ_B\,|\Phi^+\rangle\,\|.\end{aligned} \tag{3.110}$$

Let us consider the first and the last norm on the right-hand side of this inequality. With the aid of inequalities (3.76) and the fact that $X_AX_B\,|\Phi^+\rangle = Z_AZ_B\,|\Phi^+\rangle = |\Phi^+\rangle$ both can be upper bounded by $\sqrt{\varepsilon_1} + \|\Phi(|\psi'\rangle\,|00\rangle) - |\mathrm{junk}'\rangle\,|\Phi^+\rangle\,\|$. Then, from the definition of the unitary operation Φ and the state $|\mathrm{junk}'\rangle$ it follows that the latter norm can be upper bounded as

$$\begin{aligned}\|\Phi(|\psi'\rangle\,|00\rangle) - |\mathrm{junk}'\rangle\,|\Phi^+\rangle\,\| \leq & \frac{1}{4}\Big(\|X_A(\mathbb{1}-Z_A)(\mathbb{1}+\widetilde{Z}_B)\,|\psi'\rangle\,\| + \|\widetilde{X}_B(\mathbb{1}+Z_A)(\mathbb{1}-\widetilde{Z}_B)\,|\psi'\rangle\,\| \\ & + \|X_A\widetilde{X}_B(\mathbb{1}-Z_A)(\mathbb{1}-\widetilde{Z}_B)\,|\psi'\rangle - |\mathrm{junk}'\rangle\,\|\Big).\end{aligned} \tag{3.111}$$

To upper bound the first two norms in (3.111) we first exploit inequalities (3.76) and (3.77) which allow us to "convert" $\widetilde{Z}_B$ to Z_B and then Z_B to Z_A introducing an error of $8\sqrt{\varepsilon_1}$, and then we use the fact that $(\mathbb{1}+Z'_A)(\mathbb{1}-Z'_A) = 0$. To upper bound the last norm in (3.111) we first use the anticommutation relation (3.92) which leads us to

$$\|X_A\widetilde{X}_B(\mathbb{1}-Z_A)(\mathbb{1}-\widetilde{Z}_B)\,|\psi'\rangle - |\mathrm{junk}'\rangle\,\| \leq 2\omega_{\mathrm{ev}}(n) + 2\|X_A\widetilde{X}_B(\mathbb{1}-\widetilde{Z}_B)\,|\psi'\rangle - (\mathbb{1}+\widetilde{Z}_B)\,|\psi'\rangle\,\|.$$

One then uses again inequalities (3.76) and (3.77) in order to "convert" $\widetilde{Z}_B$ to Z_B and then Z_B to Z_A. This gives

$$\begin{aligned}\|X_A\widetilde{X}_B(\mathbb{1}-Z_A)(\mathbb{1}-\widetilde{Z}_B)\,|\psi'\rangle - |\mathrm{junk}'\rangle\,\| \leq\; & 2\omega_{\mathrm{ev}}(n) + 8\sqrt{\varepsilon_1} \\ & + 2\|X_A\widetilde{X}_B(\mathbb{1}-Z_A)\,|\psi'\rangle - (\mathbb{1}+Z_A)\,|\psi'\rangle\,\|.\end{aligned}$$

After applying (3.92) and then (3.76) and (3.77), one finally arrives at

$$\|X_A\widetilde{X}_B(\mathbb{1}-Z_A)(\mathbb{1}-\widetilde{Z}_B)\,|\psi'\rangle - |\mathrm{junk}'\rangle\,\| \leq 4\omega_{\mathrm{ev}}(n) + 16\sqrt{\varepsilon_1}.$$

Taking all this into account, we have that

$$\|\Phi(|\psi'\rangle|00\rangle)-|\mathrm{junk}'\rangle|\Phi^{+}\rangle\|\leq 6\sqrt{\varepsilon_1}+\omega_{\mathrm{ev}}(n). \tag{3.112}$$

Let us now pass to the second norm in (3.110) and notice that by using inequality (3.76) and the fact that $Z_B|\Phi^{+}\rangle=Z_A|\Phi^{+}\rangle$, it can be upper bounded in the following way

$$\begin{aligned}\|\Phi(X_A'Z_B'|\psi'\rangle|00\rangle)-|\mathrm{junk}'\rangle X_AZ_B|\Phi^{+}\rangle\|\leq\sqrt{\varepsilon_1}+\frac{1}{4}\Big(&\|(\mathbb{1}+Z_A')(\mathbb{1}+\widetilde{Z}_B)X_A'Z_A'|\psi'\rangle\|\\&+\|X_A'\widetilde{X}_B(\mathbb{1}+Z_A')(\mathbb{1}+\widetilde{Z}_B)X_A'Z_A'|\psi'\rangle\|\Big)\\&+\|X_A'(\mathbb{1}-Z_A')(\mathbb{1}+\widetilde{Z}_B)X_A'Z_A'|\psi'\rangle-|\mathrm{junk}'\rangle\|\\&+\|\widetilde{X}_B(\mathbb{1}+Z_A')(\mathbb{1}-\widetilde{Z}_B)X_A'Z_A'|\psi'\rangle+|\mathrm{junk}'\rangle\|\Big).\end{aligned} \tag{3.113}$$

Let us consider the first two norms appearing on the right-hand side of (3.113). Exploiting the anticommutation relation (3.92) and then inequalities (3.76) and (3.77) to convert $\widetilde{Z}_B$ to Z_A, we can bound each of these norms by $4\sqrt{\varepsilon_1}+2\omega_{\mathrm{ev}}(n)$. Using then the inequality (3.92), the third term is not larger than $2\omega_{\mathrm{ev}}(n)$. To bound the fourth term in (3.113), let us use the fact that $\|\mathbb{1}+Z_A'\|\leq 2$ to write

$$\|\widetilde{X}_B(\mathbb{1}+Z_A')(\mathbb{1}-\widetilde{Z}_B)X_A'Z_A'|\psi'\rangle-|\mathrm{junk}'\rangle\|\leq 2\|\widetilde{X}_B(\mathbb{1}-\widetilde{Z}_B)X_A'Z_A'|\psi'\rangle-(\mathbb{1}+\widetilde{Z}_B)|\psi'\rangle\|.$$

Subsequent usage of inequalities (3.76) and (3.77) to $\widetilde{Z}_B$ and $\widetilde{X}_B$ gives

$$\begin{aligned}\|\widetilde{X}_B(\mathbb{1}+Z_A')(\mathbb{1}-\widetilde{Z}_B)X_A'Z_A'|\psi'\rangle-|\mathrm{junk}'\rangle\|&\leq\\&\leq 16\sqrt{\varepsilon_1}+2\|X_A'Z_A'(\mathbb{1}-Z_A')X_A'|\psi'\rangle-(\mathbb{1}+Z_A')|\psi'\rangle\|,\end{aligned}$$

which after double application of (3.92) yields

$$\|\widetilde{X}_B(\mathbb{1}+Z_A')(\mathbb{1}-\widetilde{Z}_B)X_A'Z_A'|\psi'\rangle-|\mathrm{junk}'\rangle\|\leq 16\sqrt{\varepsilon_1}+2\omega_{\mathrm{ev}}(n).$$

This together with previous estimations finally implies that

$$\|\Phi(X_A'Z_A'|\psi'\rangle|00\rangle)-|\mathrm{junk}'\rangle X_AZ_B|\Phi^{+}\rangle\|\leq 7\sqrt{\varepsilon_1}+2\omega_{\mathrm{ev}}(n).$$

In a fully analogous way one can estimate the third term on the right-hand side of (3.110)

$$\|\Phi(Z_A'X_B'|\psi'\rangle|00\rangle)-|\mathrm{junk}'\rangle Z_AX_B|\Phi^{+}\rangle\|\leq 7\sqrt{\varepsilon_1}+2\omega_{\mathrm{ev}}(n).$$

By plugging all these terms into (3.110) and then the resulting inequality together with (3.109) into (3.108), one obtains

$$\|\Phi(A_i'B_j'|\psi'\rangle|00\rangle)-|\mathrm{junk}'\rangle A_iB_j|\Phi^{+}\rangle\|\leq 28\sqrt{\varepsilon_1}+6\omega_{\mathrm{ev}}(n)+g_{\mathrm{ev}}+h_{\mathrm{ev}}. \tag{3.114}$$

The terms from (3.102) can be treated in almost exactly the same way, giving

$$\|\Phi(A_i'|\psi'\rangle|00\rangle)-|\mathrm{junk}'\rangle A_i|\Phi^+\rangle\|\leq 12\sqrt{\varepsilon_1}+3\omega_{\mathrm{ev}}(n)+g_{\mathrm{ev}}, \tag{3.115}$$

while the estimation of the corresponding expression from (3.102) follows from the application of inequality (3.76) to (3.115), meaning that an additional error of $\sqrt{\varepsilon_1}$ has to be taken into account, which gives

$$\|\Phi(B_j'|\psi'\rangle|00\rangle)-|\mathrm{junk}'\rangle B_j|\Phi^+\rangle\|\leq 13\sqrt{\varepsilon_1}+3\omega_{\mathrm{ev}}(n)+h_{\mathrm{ev}}. \tag{3.116}$$

Finally, the case of $A_i'=B_j'=\mathbb{1}$ has already been derived in (3.112).

The distance between the normalized state $|\mathrm{junk}\rangle$ and the unnormalized one $|\mathrm{junk}'\rangle$ is estimated in Lemma 3.4 to be

$$\|\,|\mathrm{junk}\rangle-|\mathrm{junk}'\rangle\,\|\leq\left(\frac{1}{2}+\sqrt{2}\right)\sqrt{\varepsilon_1}+\omega', \tag{3.117}$$

where ω' is equal to ω_{ev} for an even number of inputs.

In order to obtain inequalities (3.101) and complete the proof we use the triangle inequality for the vector norm to write

$$\begin{aligned}\|\Phi(A_i'B_j'|\psi'\rangle|00\rangle)-|\mathrm{junk}\rangle A_iB_j|\Phi^+\rangle\| \quad\leq\quad & \|\Phi(A_i'B_j'|\psi'\rangle|00\rangle)-|\mathrm{junk}'\rangle A_iB_j|\Phi^+\rangle\| \\ & +\|\,|\mathrm{junk}\rangle-|\mathrm{junk}'\rangle\,\|,\end{aligned} \tag{3.118}$$

and then apply the previously determined inequalities (3.112), (3.114), (3.115), (3.116) and (3.117). All terms contributing to the functions $f(\varepsilon,n)$, $f_{B_j}(\varepsilon,n)$, $f_{A_i}(\varepsilon,n)$ and $f_{ij}(\varepsilon,n)$ scale at most as $O(n^2\sqrt{\varepsilon})$. □

3.4 Randomness certification with the chained Bell inequalities

It has been shown in Ref. [DPA13] that by exploiting the symmetry properties of the chained Bell inequality, one can certify two bits of randomness when the maximum quantum violation of this inequalities are obtained, provided this maximal quantum violation is unique. However, a proof of the latter fact has not been known so far. Here, we complete the result of Ref. [DPA13].

Let us now provide an alternative way of certifying two bits of perfect randomness with the aid of the chained Bell inequality. For this purpose, we consider the following modification of the chained Bell inequality

$$\widetilde{I}_{\mathrm{ch}}^{n}:=\mathscr{I}_{\mathrm{ch}}^{n}+\langle A_1'B_{n+1}'\rangle\leq 2n-1 \tag{3.119}$$

in which Alice, as before, can measure one of n observables A'_i while Bob has $n+1$ observables B'_i at his disposal, where n is assumed to be even. It is not difficult to see that the maximal quantum violation of this inequality amounts to $\widetilde{\beta}_Q^n = \beta_Q^n + 1$.

Let us now assume that $|\psi'\rangle$ and A'_i and B'_i are the state and the measurements maximally violating (3.119). Denoting then by $\widetilde{\mathscr{B}}_{ch}^n = \mathscr{B}_{ch}^n + A'_1 \otimes B'_{n+1}$ the corresponding Bell operator, one has $\langle\psi'|(\widetilde{\beta}_Q^n \mathbb{1} - \widetilde{\mathscr{B}}_{ch}^n)|\psi'\rangle = 0$, which, owing to the fact that $|\psi'\rangle$ also violates maximally the chained Bell inequality and that β_Q^n is its maximal quantum violation, simplifies to $0 = \langle\psi'|(\mathbb{1} - A'_1 \otimes B'_{n+1})|\psi'\rangle = (1/2)\langle\psi'|(\mathbb{1} - A'_1 \otimes B'_{n+1})^2|\psi'\rangle$, where the second equality is a consequence of the fact that A'_1 and B'_{n+1} are unitary and hermitian. This implies that

$$A'_1\,|\psi\rangle = B'_{n+1}\,|\psi\rangle\,. \tag{3.120}$$

This property implies in particular that $\langle B'_{n+1}\rangle = \langle A'_1\rangle$, which, taking into account the fact that for the maximal quantum violation of the chained Bell inequality $\langle A'_i\rangle = 0$ for any $i = 1,\ldots,n$, implies $\langle B'_{n+1}\rangle = 0$. In a quite analogous way we can now prove that the expectation value $\langle A'_{n/2+1}B'_{n+1}\rangle = \langle\psi'|A'_{n/2+1} \otimes B'_{n+1}|\psi'\rangle$ vanishes. Exploiting Eq. (3.120), we can rewrite it as $\langle\psi'|A'_{n/2+1} \otimes B'_{n+1}|\psi'\rangle = \langle\psi'|A'_{n/2+1}A'_1|\psi'\rangle$. Then, due to the fact that the expectation value $\langle\psi'|A'_{n/2+1} \otimes B'_{n+1}|\psi'\rangle$ is real and both operators $A'_{n/2+1}$ and B'_{n+1} are hermitian, which means that $\langle\psi'|A'_{n/2+1}A'_1|\psi'\rangle = \langle\psi'|A'_1A'_{n/2+1}|\psi'\rangle$, this can be further rewritten as

$$\langle A'_{n/2+1}B'_{n+1}\rangle = \frac{1}{2}\langle\psi'|\{A'_1, A'_{\frac{n}{2}+1}\}|\psi'\rangle. \tag{3.121}$$

We have already proven that if $|\psi'\rangle$ and A'_i and B'_i violate maximally the chained Bell inequality, then $\{A'_1, A'_{n/2+1}\}\,|\psi'\rangle = 0$ which implies that $\langle A'_{n/2+1}B'_{n+1}\rangle = 0$, which together with $\langle A'_1\rangle = \langle B'_{n+1}\rangle = 0$ mean finally that

$$p(a,b|A'_{\frac{n}{2}+1}, B'_{n+1}) = \frac{1}{4} \tag{3.122}$$

with $a,b = 0,1$. All this proves that any probability distribution $p(a,b|A'_i,B'_j)$ with $i = 1,\ldots,n$ and $j = 1,\ldots,n+1$ maximally violating the modified chained Bell inequality (3.119) is such that all outcomes of the pair of measurements $A'_{n/2+1}, B'_{n+1}$ are equiprobable (3.122) and thus perfectly random, meaning that (3.119) certifies two bits of perfect randomness.

The intuition behind the above approach is very simple. At the maximal quantum violation of (3.119) the measurement B'_{n+1} must be "parallel" to A'_1 [cf. Eq. (3.120)]. Therefore it is "orthogonal" to $A'_{n/2+1}$ as the latter is orthogonal to A'_1, meaning that $\langle A'_{n/2+1}B'_{n+1}\rangle = 0$ which is basically what we need. It is worth noticing that in the even n case all pairs $A'_{1+i},A'_{n/2+i}$ with $i = 1,\ldots,n/2-1$ of Alice's observables are orthogonal, and therefore our argument can be extended to any pair $A'_{n/2+i},B'_{n+1}$, that is, $\langle A'_{n/2+i},B'_{n+1}\rangle = 0$ provided the Bell inequality $\mathscr{I}^n_{\mathrm{ch}} + \langle A'_{n/2+i}B'_{n+1}\rangle \leq 2n-1$ is maximally violated. Unfortunately, this approach does not work in the odd n case as no pair of observables at Alice's or Bob's sides are orthogonal.

3.5 Discussion

In this chapter we developed a scheme for self-testing the maximally entangled state of two qubits using the chained Bell inequalities. Since our results hold for any number of inputs, this allows one to self-test measurements on the whole XZ plane of the Bloch sphere. Some of the previous self-testing techniques found an application for blind quantum computation protocols (See [RUV13]). The fact that chained Bell inequalities involve and certify a quite large large class of measurements makes this self-testing protocol a good candidate for some future application in blind quantum computation processes. Beyond their interest as a protocol in quantum information processing, our results also have fundamental implications, since they prove the uniqueness of the maximal violation of the chained Bell inequalities. In Ref. [DPA13], this property was assumed to be true to argue maximal randomness certification in Bell tests: with our proof, their results are now confirmed. Contrary to the expectations, when increasing the number of measurements, the robustness of our protocol diminishes. An interesting open question is to see whether it is possible to improve this scaling. Another open question concerns chained Bell inequalities with more outcomes: can they also be useful for self-testing? If so, one could also make use of these results for certifying random *dits* in systems of dimension larger than two.

Chapter 4

Self-testing multipartite quantum states

Most of the currently known self-testing protocols are tailored to bipartite states, leaving the multipartite scenario rather unexplored. In this chapter, we extend the class of multipartite states that can be self-tested, by investigating a simple approach that exploits the well-understood self-testing of two-qubit states. This is done by combining projections to two-qubit spaces and then exploiting maximal violation of tilted CHSH inequalities. Using this potentially unifying approach, we show self-testing of all Dicke states (Section 4.4) and partially entangled GHZ states with only two measurements per party. We also show that our method efficiently applies also to self-testing of graph states (Section 4.5), previously known only through stabilizer state methods, with a slight improvement in the number of measurement settings per party. Finally we provide the first self-testing result for a class of multipartite qudit states, by showing that all multipartite qudit states which possess a Schmidt decomposition can be self-tested, with at most four measurements per party (Section 4.2).

4.1 Preliminaries

Before passing to the concrete results let us fix the notation and recall some relevant previous results. Consider N non-communicating parties sharing some N-partite state $|\psi'\rangle$. On its share of this state, a party i can perform one of several projective measurements $\{M'^{a_i}_{x_i,i}\}_{a_i}$, labelled by $x_i \in \mathscr{X}_i$, with possible outcomes $a_i \in \mathscr{A}_i$. Here $\mathscr{X}_i$ and $\mathscr{A}_i$ stand for finite alphabets of possible questions and answers for party i. The experiment is characterized by a collection of conditional probabilities $\{p(a_1,\ldots,a_N|x_1,\ldots,x_N) : a_i \in \mathscr{A}_i\}_{x_i \in \mathscr{X}_i}$, where

$$p(a_1,\ldots,a_N|x_1,\ldots,x_N) = \langle\psi'|M'^{a_1}_{x_1,1} \otimes \ldots \otimes M'^{a_N}_{x_N,N}|\psi'\rangle \tag{4.1}$$

is the probability of obtaining outputs $a_1,\dots,a_N$ upon performing the measurements $x_1,\dots,x_N$[1]. We refer to this as a *correlation*. It is sometimes convenient to describe correlations with the aid of standard correlators, where instead of measurement operators $M_{x_i}^{a_i}$ one uses Hermitian observables with eigenvalues ± 1. Now, analogously to bipartite self-testing (2.5) we can define multipartite self-testing in the following way.

Definition 4.1. *We say that a correlation $\{p(a_1,\dots,a_N|x_1,\dots,x_N) : a_i \in \mathscr{A}_i\}_{x_i\in\mathscr{X}_i}$ self-tests the state $|\psi\rangle$ and measurements $\{M_{x_i,i}^{a_i}\}_{a_i}$, $i=1,\dots,N$, if for any state and measurements $|\psi'\rangle$ and $\{M'^{a_i}_{x_i,i}\}_{a_i}$, $i=1,\dots,N$, reproducing the correlation, there exists a local isometry $\Phi=\Phi_1\otimes\ldots\otimes\Phi_N$ such that*

$$\Phi(M'^{a_1}_{x_1,1}\otimes\ldots\otimes M'^{a_N}_{x_N,N}|\psi'\rangle) = |\text{junk}\rangle\otimes(M^{a_1}_{x_1,1}\otimes\ldots\otimes M^{a_N}_{x_N,N}|\psi\rangle). \tag{4.2}$$

where $|\text{junk}\rangle$ is some auxiliary state representing unimportant degrees of freedom.

In the bipartite scenario (as we saw in Subsection 2.5.2) existence of an isometry obeying (4.2) can be proven solely from the maximal violation of some Bell inequality. Moreover, all two-qubit pure entangled states can be self-tested with a one-parameter class of tilted CHSH Bell inequalities [BP15] given by

$$\alpha\langle A_0\rangle+\langle A_0B_0\rangle+\langle A_0B_1\rangle+\langle A_1B_0\rangle-\langle A_1B_1\rangle\leq 2+\alpha, \tag{4.3}$$

where $\alpha\geq 0$ and A_i and B_i are observables with outcomes ±1 measured by the parties. Note that for $\alpha=0$, Eq. (4.3) reproduces the well-known CHSH Bell inequality [CHSH69]. For further purposes let us briefly recall this result. Here σ_Z and σ_X are the standard Pauli matrices.

Lemma 4.1 ([BP15])**.** *Suppose a bipartite state $|\psi'\rangle$ and dichotomic observables A_i and B_i achieve the maximal quantum violation of the tilted CHSH inequality (4.3) $\sqrt{8+2\alpha^2}$, for some α. Let $\theta,\mu\in(0,\pi/2)$ be such that* $\sin 2\theta=\sqrt{(4-\alpha^2)/(4+\alpha^2)}$ *and* $\mu=\arctan\sin 2\theta$. *Let $Z_A=A_0$, $X_A=A_1$. Let Z_B^* and X_B^* be respectively $(B_0+B_1)/2\cos\mu$ and $(B_0-B_1)/2\sin\mu$, but with all zero eigenvalues replaced by one, and define $Z_B=Z_B^*|Z_B^*|^{-1}$ and $X_B=X_B^*|X_B^*|^{-1}$. Then, we have*

$$Z_A|\psi'\rangle=Z_B|\psi'\rangle, \tag{4.4}$$

$$\cos\theta X_A(\mathbb{1}-Z_A)|\psi'\rangle=\sin\theta X_B(\mathbb{1}+Z_A)|\psi'\rangle, \tag{4.5}$$

$$\{X_A,Z_A\}|\psi'\rangle=0,\qquad \{X_B,Z_B\}|\psi'\rangle=0 \tag{4.6}$$

Moreover, there exists a local isometry Φ such that $\Phi(A_i\otimes B_j|\psi'\rangle)=|\text{junk}\rangle\otimes(\tilde{A}_i\otimes\tilde{B}_j)|\psi_\theta\rangle$, where $|\psi_\theta\rangle=\cos\theta|00\rangle+\sin\theta|11\rangle$, and $\tilde{A}_0=\sigma_Z$, $\tilde{A}_1=\sigma_X$, and $\tilde{B}_{0/1}=\cos\mu\sigma_Z\pm\sin\mu\sigma_X$.

As in the previous Chapter a typical construction of the isometry Φ is the one encoding the SWAP gate, as illustrated in Fig. 4.1.

[1] We take the parties' measurements to be projective, invoking Naimark's dilation theorem. We take the joint state to be pure for ease of exposition, but we emphasize that all of our proofs hold analogously starting from a joint mixed state.

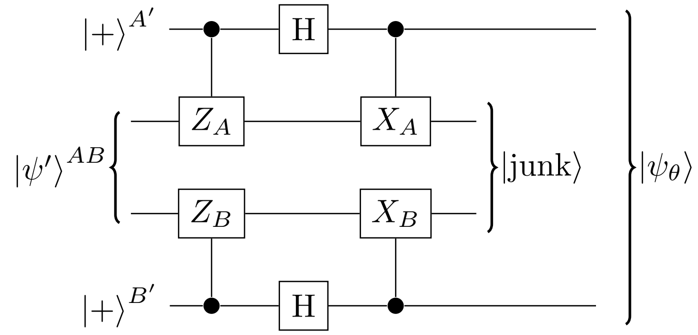

Figure 4.1: Example of a circuit that takes as input a state $|\psi'\rangle$ satisfying (4.4)-(4.5), adds two ancillas, each in $|+\rangle$, and outputs the state $|\psi_\theta\rangle$ in tensor product with an auxiliary state $|\text{junk}\rangle$. Here H is the usual Hadamard gate.

Our aim in this chapter is to exploit the above result to develop methods for self-testing multipartite entangled quantum states. Given an N-partite entangled state $|\psi'\rangle$, the idea is that $N-2$ chosen parties perform local measurements on their shares of $|\psi'\rangle$ and the remaining two parties check whether the projected state they share violates maximally (4.3) for the appropriate α (we can think of this as a sub-test). This procedure is repeated for various subsets of $N-2$ parties until the correlations imposed are sufficient to characterize the state $|\psi\rangle$. This approach is inspired by Ref. [Wu+14], which shows that any state in the class $(|100\rangle + |101\rangle + \alpha\,|001\rangle)/\sqrt{2+\alpha^2}$, containing the three-qubit W state, can be self-tested in this way. We will show that this approach can be generalized in order to self-test new (and old) classes of multipartite states. The main challenge is to show that all the sub-tests of different pairs of parties are compatible. To be more precise, for a generic state there will always be a party which will be involved in several different sub-tests and, in principle, will be required to use different measurements to pass the different tests. Consequently, isometries (Fig. 4.1) corresponding to different sub-tests are in principle constructed from different observables. However, a single isometry is required in order to self-test the global state. Overcoming the problem of building a single isometry from several different ones is the key step to achieve a valid self-test for multipartite states. For states that exhibit certain symmetries, this can be done efficiently with few measurements. We leave for future work the exploration for states that do not have any particular symmetry.

In the N-partite scenario, parties will be denoted by numbers from 1 to N and measurement observables by capital letters with a superscript denoting the party. For a two-outcome observable W, we denote by $W^{(\pm)} = (\mathbb{1} \pm W)/2$ the projectors onto the ± 1 eigenspaces. We use the notation $\lfloor a \rfloor$ to denote the biggest integer n such that $n \leq a$, while $\lceil a \rceil$ is the smallest n such that $n \geq a$.

4.2 All multipartite entangled qudit Schmidt states

While in the bipartite setting all states admit a Schmidt decomposition (2.2), in the general multipartite setting this is not the case. We refer to those multipartite states that admit a Schmidt decomposition as Schmidt states. These, up to a local unitary, can be written in the form

$$|\psi_s\rangle = \sum_{j=0}^{d-1} c_j \,|j\rangle^{\otimes N} \tag{4.7}$$

where $0 < c_j < 1$ for all i and $\sum_{j=0}^{d-1} c_j^2 = 1$.

The proof that all multipartite entangled Schmidt states can be self-tested exploits the ideas from Refs. [YN13] and [CGS17]. The main building block of the proof is our novel self-testing result for partially entangled GHZ states. Thus, we proceed by first proving a self-testing theorem for multipartite partially entangled qubit GHZ states.

4.2.1 Multipartite partially entangled GHZ states

Multipartite qubit Schmidt states, also known as partially entangled GHZ states, are of the form

$$|\mathrm{GHZ}_N(\theta)\rangle = \cos\theta\,|0\rangle^{\otimes N} + \sin\theta\,|1\rangle^{\otimes N} \tag{4.8}$$

where $\theta \in (0, \pi/4]$ and $|\mathrm{GHZ}_N(\pi/4)\rangle = |\mathrm{GHZ}_N\rangle$ is the standard N-qubit GHZ state. The form of this state is such that if any subset of $N-2$ parties performs a σ_{X} measurement, the collapsed state shared by the remaining two parties is $\cos\theta\,|00\rangle \pm \sin\theta\,|11\rangle$, depending on the parity of the measurement outcomes. As already mentioned, these states can be self-tested with the aid of inequality (4.3), which is the main ingredient of our self-test of $|\mathrm{GHZ}_N(\theta)\rangle$.

Theorem 5. *Let $|\psi'\rangle$ be an N-partite state, and let $A_{0,i}, A_{1,i}$ be a pair of binary observables for the i-th party, for $i = 1,\ldots,N$. Suppose the following correlations are satisfied:*

$$\langle\psi'|A_{0,i}^{(+)}|\psi'\rangle = \langle\psi'|A_{0,i}^{(+)}A_{0,j}^{(+)}|\psi'\rangle = \cos^2\theta, \qquad \forall i,j \in \{1,\ldots,N-1\} \tag{4.9}$$

$$\langle\psi'|\prod_{i=1}^{N-2} A_{1,i}^{(a_i)}|\psi'\rangle = \frac{1}{2^{N-2}}, \qquad \forall a \in \{+,-\}^{N-2} \tag{4.10}$$

$$\langle\psi'|\prod_{i=1}^{N-2} A_{1,i}^{(a_i)}(\alpha A_{0,N-1} + A_{0,N-1}A_{0,N} + A_{0,N-1}A_{1,N} + (-1)^{h(a)}A_{1,N-1}A_{0,N} \tag{4.11}$$

$$-(-1)^{h(a)}A_{1,N-2}A_{1,N-1})\,|\psi'\rangle = \frac{\sqrt{8+2\alpha^2}}{2^{N-2}}, \qquad \forall a \in \{+,-\}^{N-2} \tag{4.12}$$

where $h(a)$ denotes the parity of the number of "$-$" in a, and $\alpha = 2\cos 2\theta/\sqrt{1+\sin^2 2\theta}$. Let μ be such that $\tan\mu = \sin 2\theta$. Define $Z_i = A_{0,i}$ and $X_i = A_{1,i}$, for $i = 1,\dots,N-1$. Then, let $Z'_N = (A_{0,N} + A_{1,N})/2\cos\mu$, and let Z^*_N be Z'_N with zero eigenvalues replaced by 1. Define $Z_N = Z^*_N|Z^*_N|^{-1}$. Define X_N similarly starting from $X'_N = (A_{0,N} - A_{1,N})/2\sin\mu$. Then,

$$Z_1\,|\psi'\rangle = \cdots = Z_N\,|\psi'\rangle\,, \tag{4.13}$$

$$X_1\cdots X_N(I - Z_1)\,|\psi'\rangle = \tan\theta(I + Z_1)\,|\psi'\rangle\,. \tag{4.14}$$

Before providing the formal proof let us give an intuitive understanding of the correlations given above. The first equation (4.9) defines the existence of one measurement observable, whose marginal carries the information of angle θ. The straightforward consequence of it is Eq. (4.13), which is analogue to Eq. (4.4). On the other hand, eq. (4.10) involves a different measurement observable with zero marginal, while Eq. (4.11) shows that when the first $N-2$ parties perform this zero marginal measurement the remaining two parties maximally violate the corresponding tilted CHSH inequality, i.e. the reduced state is self-tested to be the partially entangled pair of qubits. Eq. (4.14) is analogue to Eq. (4.5).

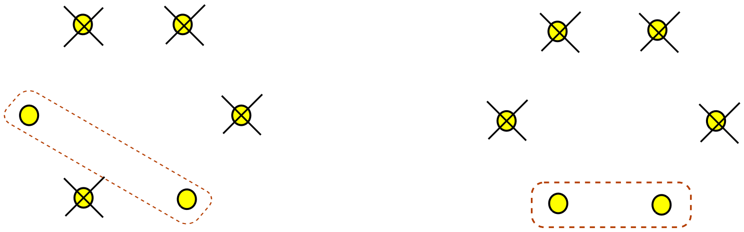

Figure 4.2: Two steps in the self-test of five-partite partially entangled GHZ-state. The crossed qubits are measured in a suitable basis so that the two remaining qubits are projected to one of the partially entangled pairs of qubits $\cos\theta\,|00\rangle \pm \sin\theta\,|11\rangle$. The corresponding pair can be self-tested by using the tilted CHSH inequality. In the second step the procedure is repeated for different qubits being measured, thus preparing a different pair of qubits in a state that can be self-tested.

Proof. For ease of exposition, we prove the Theorem in the case $N = 4$, with the extension to general N being immediate.

Let $A_0, A_1, B_0, B_1, C_0, C_1, D_0, D_1$, be the pairs of observables for the four parties. For an observable D, let $P^a_D = [\mathbb{1} + (-1)^a D]/2$, and for brevity let c_θ and s_θ denote respectively $\cos\theta$ and $\sin\theta$. For clarity, we recall the correlations from Theorem 5, for the case $N = 4$:

$$\langle\psi'|P^0_{A_0}|\psi'\rangle = \langle\psi'|P^0_{B_0}|\psi'\rangle = \langle\psi'|P^0_{C_0}|\psi'\rangle = \langle\psi'|P^0_{A_0}P^0_{C_0}|\psi'\rangle = \langle\psi'|P^0_{B_0}P^0_{C_0}|\psi'\rangle = c^2_\theta, \tag{4.15a}$$

$$\langle\psi'|P^a_{A_1}P^b_{B_1}|\psi'\rangle = \frac{1}{4}, \tag{4.15b}$$

$$\langle\psi'|P^a_{A_1}P^b_{B_1}\big(\alpha C_0 + C_0D_0 + C_0D_1 + (-1)^{a+b}(C_1D_0 - C_1D_1)\big)|\psi'\rangle = \frac{\sqrt{8+2\alpha^2}}{4}, \tag{4.15c}$$

where $\tan 2\theta = \sqrt{\frac{2}{\alpha^2} - \frac{1}{2}}$. The last two equations have to hold for all $a, b \in \{0,1\}$. Eqs. (4.15a) imply, by Cauchy-Schwartz inequality, that

$$P^0_{A_0}|\psi'\rangle = P^0_{B_0}|\psi'\rangle = P^0_{C_0}|\psi'\rangle \tag{4.16}$$

and consequently

$$P^1_{A_0}|\psi'\rangle = P^1_{B_0}|\psi'\rangle = P^1_{C_0}|\psi'\rangle. \tag{4.17}$$

Notice that Eq. (4.15b) implies $\|P^a_{A_1}P^b_{B_1}|\psi'\rangle\| = 1/2$, for $a, b \in \{0,1\}$, and that the equations in (4.15c) describe maximal violations of tilted CHSH inequalities by the normalized state $2P^a_{A_1}P^b_{B_1}|\psi'\rangle$, for $a, b \in \{0,1\}$ (the ones for $a \oplus b = 1$ are tilted CHSH inequalities upon relabelling $D_1 \to -D_1$).

Let μ be such that $\tan\mu = s_{2\theta}$. Define $X_A := A_1, X_B := B_1$ and $X_C := C_1$. Then, let $Z'_D = (D_0 + D_1)/2\cos\mu$, and let Z^*_D be Z'_D where we have replaced the zero eigenvalues with 1. Define $Z_D = Z^*_D|Z^*_D|^{-1}$. Define X_D similarly starting from $X'_D = (D_0 - D_1)/2\cos\mu$. Let $P^a_{Z_D} = [\mathbb{1} + (-1)^a Z_D]/2$. The maximal violations of tilted CHSH from (4.15c) imply, thanks to Lemma 4.1, that

$$P^a_{C_0} = P^a_{Z_D}, \quad \text{for } a \in \{0,1\}, \tag{4.18}$$

$$s_\theta P^a_{A_1}P^b_{B_1}X_CX_DP^0_{C_0}|\psi'\rangle = (-1)^{a+b}c_\theta P^a_{A_1}P^b_{B_1}P^1_{C_0}|\psi'\rangle, \text{ for } a, b \in \{0,1\}. \tag{4.19}$$

If we introduce notation $X_A = A_1, X_B = B_1$ and $X_C = C_1$, then

$$\begin{aligned}
X_AX_BX_CX_DP^1_{A_0}|\psi'\rangle &= (P^0_{A_1} - P^1_{A_1})(P^0_{B_1} - P^1_{B_1})X_CX_DP^1_{C_0}|\psi'\rangle \\
&= P^0_{A_1}P^0_{B_1}X_CX_DP^1_{C_0}|\psi'\rangle - P^0_{A_1}P^1_{B_1}X_CX_DP^1_{C_0}|\psi'\rangle - P^1_{A_1}P^0_{B_1}X_CX_DP^1_{C_0}|\psi'\rangle \\
&\quad + P^1_{A_1}P^1_{B_1}X_CX_DP^1_{C_0}|\psi'\rangle \qquad (4.20) \\
&= \frac{s_\theta}{c_\theta}P^0_{A_1}P^0_{B_1}P^0_{A_0}|\psi'\rangle + \frac{s_\theta}{c_\theta}P^0_{A_1}P^1_{B_1}P^0_{A_0}|\psi'\rangle + \frac{s_\theta}{c_\theta}P^0_{A_1}P^1_{B_1}P^0_{A_0}|\psi'\rangle \\
&\quad + \frac{s_\theta}{c_\theta}P^1_{A_1}P^1_{B_1}P^0_{A_0}|\psi'\rangle \\
&= \frac{s_\theta}{c_\theta}P^0_{A_0}|\psi'\rangle, \qquad (4.21)
\end{aligned}$$

where we used equation (4.19) to obtain the third line, and $\sum_{a,b\in\{0,1\}} P^a_{A_1} P^b_{B_1} = \mathbb{1}$ to obtain the last. Conditions (4.13) and (4.14) of Theorem 5 follow immediately from the above.

□

As a Corollary, note that the correlations from Theorem 5 self-test the state $|\mathrm{GHZ}_N(\theta)\rangle$.

Corollary 5.1. *Let $|\psi'\rangle$ be an N-partite state, and let $A_{0,i}, A_{1,i}$ be a pair of binary observables for the ith party, for $i = 1,\dots,N$. Suppose they satisfy the correlations of Theorem 5. Then, there exists a local isometry Φ such that*

$$\Phi(|\psi'\rangle) = |\mathrm{junk}\rangle\,|\mathrm{GHZ}_N(\theta)\rangle \tag{4.22}$$

Proof: This follows as a special case ($d = 2$) of Lemma 5.1 stated below, upon defining $P_i^{(k)} = [\mathbb{1} + (-1)^k Z_i]/2$, for $k \in \{0,1\}$.

As one can expect, the ideal measurements achieving these correlations are: $A_{0,i} = \sigma_\mathrm{Z}$, $A_{1,i} = \sigma_\mathrm{X}$, for $i = 1,\dots,N-1$, and $A_{0,N} = \cos\theta\sigma_\mathrm{Z} + \sin\theta\sigma_\mathrm{X}$, $A_{1,N} = \cos\theta\sigma_\mathrm{Z} - \sin\theta\sigma_\mathrm{X}$. We refer to the correlations achieved by these ideal measurements as the *ideal correlations* for multipartite entangled GHZ states.

4.2.2 All multipartite entangled qudit Schmidt states

The generalisation of Theorem 5 to all multipartite qudit Schmidt states is then an adaptation of the proof from Ref. [CGS17] to the multipartite case, with the difference that it uses as a building block the $|\mathrm{GHZ}_N(\theta)\rangle$ self-test that we just developed, instead of the tilted CHSH inequality.

We begin by stating a straightforward generalisation to the multipartite setting of the criterion from [YN13] which gives sufficient conditions for self-testing a Schmidt state. Then, our proof that all multipartite entangled qudit Schmidt states can be self-tested goes through showing the existence of operators satisfying the conditions of such criterion.

Lemma 5.1 (Generalisation of criterion from [YN13]). *Let $|\psi'\rangle$ be a N-partite quantum state. Suppose there exist sets of unitaries $\{X_l^{(k)}\}_{k=0}^{d-1}$, where the subscript $l \in \{1,\dots,N\}$ indicates that the operator acts on the system of the l-th party, and sets of projections $\{P_l^{(k)}\}_{k=0}^{d-1}$, that are complete and orthogonal for $l = 1,\dots,N-1$ but not necessarily such for $l = N$, and they satisfy:*

$$P_1^{(k)}|\psi'\rangle = \ldots = P_N^{(k)}|\psi'\rangle, \tag{4.23}$$

$$X_1^{(k)}\ldots X_N^{(k)} P_1^{(k)}|\psi'\rangle = \frac{c_k}{c_0} P_1^{(0)}|\psi'\rangle \tag{4.24}$$

for all $k = 1,\dots,N$. Then, there exists a local isometry Φ such that $\Phi(|\psi'\rangle) = |junk\rangle \otimes |\psi_s\rangle$.

We explicitly construct a local isometry Φ such that $\Phi(|\psi'\rangle) = |\text{junk}\rangle \otimes |\psi_s\rangle$ for any Schmidt state $|\psi_s\rangle = \sum_{j=0}^{d-1} c_j \, |j\rangle^{\otimes N}$, where $0 < c_j < 1$ for all j and $\sum_{j=0}^{d-1} c_j^2 = 1$, and $|\text{junk}\rangle$ is some auxiliary state.

Proof. Recall that $\{P_l^{(k)}\}_{k=0}^{d-1}$ are complete sets of orthogonal projections for $l = 1, \ldots, N-1$ by hypothesis. Then, notice that for $i \neq j$ we have, using condition (4.23), $P_N^{(i)} P_N^{(j)} |\psi'\rangle = P_N^{(i)} P_1^{(j)} |\psi\rangle = P_1^{(j)} P_1^{(i)} |\psi\rangle = 0$, i.e., the $P_N^{(k)}$ are "orthogonal when acting on $|\psi\rangle$".

Let $\mathscr{A}$ be the unital algebra generated by $\{P_1^{(k)}\}$. Let $\mathscr{H}' = \mathscr{A} \, |\psi'\rangle$, where $\mathscr{A} \, |\psi'\rangle = \{Q \, |\psi\rangle : Q \in \mathscr{A}\}$. Let $\tilde{P}_N^{(k)} = P_N^{(k)}|_{\mathscr{H}'}$ be the restriction of $P_N^{(k)}$ to $\mathscr{H}'$. Then, $\{\tilde{P}_N^{(k)}\}_{k=0}^{d-1}$ is a set of orthogonal projections. This is because, thanks to (4.23), one can always move the relevant operators to be in front of $|\psi\rangle$, as in the simple example

$$\tilde{P}_N^{(i)} \tilde{P}_N^{(j)} (P_1^{(k)} \, |\psi'\rangle') = P_1^{(k)} \tilde{P}_N^{(i)} \tilde{P}_N^{(j)} \, |\psi'\rangle = 0. \tag{4.25}$$

Thus, the set $\{\tilde{P}_B^{(k)}, I - P_B'\}$, where P_B' is the sum of all other projections, is a complete set of orthogonal projections.

Now, define $Z_l := \sum_{k=0}^{d-1} \omega^k P_l^{(k)}$, for $l = 1, \ldots, N-1$, and $Z_N := \sum_{k=0}^{d-1} \omega^k \tilde{P}_N^{(k)} + \mathbb{1} - \sum_{k=0}^{d-1} \tilde{P}_N^{(k)}$. In particular, the Z_l are all unitary. Notice, moreover, that $\left(\mathbb{1} - \sum_k \tilde{P}_N^{(k)}\right) |\psi'\rangle = 0$, by using (4.23) and the fact that the $\{P_l^{(k)}\}$ are complete.

Define the local isometry

$$\Phi := \bigotimes_{l=1}^{N} R_{ll'} \bar{F}_{l'} S_{ll'} F_{l'} \text{App}_l, \tag{4.26}$$

where $\text{App}_l : \mathscr{H}_l \to \mathscr{H}_l \otimes \mathscr{H}_{l'}$ is the isometry that simply appends $|0\rangle_l'$, F is the quantum Fourier transform, $\bar{F}$ is the inverse quantum Fourier transform, $R_{ll'}$ is defined so that $|\phi\rangle_l \, |k\rangle_{l'} \mapsto X_l^{(k)} \, |\phi\rangle_l \, |k\rangle_{l'} \;\forall |\phi\rangle$, and $S_{ll'}$ is defined so that $|\phi\rangle_l \, |k\rangle_{l'} \mapsto Z_l^k \, |\phi\rangle_l \, |k\rangle_{l'} \;\forall |\phi\rangle$. We compute the action of Φ on $|\psi'\rangle$. For ease of notation with drop the tildes from the $\tilde{P}_N^{(k)}$, while still referring to the new orthogonal projections.

$$\begin{aligned}
|\psi'\rangle \otimes |0\rangle^{\otimes N} &\xrightarrow{\bigotimes_l F_{l'}} \frac{1}{d^{N/2}} \sum_{k_1,\ldots,k_N} |\psi'\rangle \bigotimes_l |k_l\rangle_{l'} \\
&\xrightarrow{\bigotimes_l S_{ll'}} \frac{1}{d^{N/2}} \sum_{k_1,\ldots,k_N} \left[\prod_{i=1}^{N-1} \left(\sum_{j_i} \omega^{j_i} P_i^{(j_i)}\right)^{k_i}\right] \left(\sum_{j_N} \omega^{j_N} P_N^{(j_N)} + \mathbb{1} - \sum_k P_N^{(j_N)}\right)^{k_N} |\psi'\rangle \bigotimes_l |k_l\rangle_{l'} \\
&= \frac{1}{d^{N/2}} \sum_{k_1,\ldots,k_N} \sum_{j_1,\ldots,j_N} \prod_{i=1}^{N} \omega^{j_i k_i} P_i^{(j_i)} \, |\psi'\rangle \bigotimes_l |k_l\rangle_{l'} \\
&= \frac{1}{d^{N/2}} \sum_{k_1,\ldots,k_N} \sum_{j_1,\ldots,j_N} \prod_{i=1}^{N} \omega^{j_i k_i} P_1^{(j_i)} \, |\psi'\rangle \bigotimes_l |k_l\rangle_{l'}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{d^{N/2}} \sum_{k_1,\dots,k_N} \sum_j \omega^{j(\Sigma_i k_i)} P_1^{(j)} \left|\psi'\right\rangle \bigotimes_l \left|k_l\right\rangle_{l'} \\
&\xrightarrow{\otimes_l \bar{F}_{l'}} \frac{1}{d^N} \sum_{k_1,\dots,k_N} \sum_j \sum_{m_1,\dots,m_N} \omega^{j(\Sigma_i k_i)} \prod_r \omega^{-m_r k_r} P_1^{(j)} \left|\psi'\right\rangle \bigotimes_l \left|m_l\right\rangle_{l'} \\
&= \frac{1}{d^N} \sum_{k_1,\dots,k_N} \sum_j \sum_{m_1,\dots,m_N} \prod_i \omega^{k_i(j-m_i)} P_1^{(j)} \left|\psi'\right\rangle \bigotimes_l \left|m_l\right\rangle_{l'}
\end{aligned}
$$

$$
= \sum_j P_1^{(j)} \left|\psi'\right\rangle \otimes \left|j\right\rangle^{\otimes N} \tag{4.27}
$$

$$
\xrightarrow{\otimes_l R_{ll'}} \sum_j \left(\prod_i X_i^{(j)} \right) P_1^{(j)} \left|\psi'\right\rangle \otimes \left|j\right\rangle^{\otimes N}
$$

$$
= \sum_j \frac{c_j}{c_0} P_1^{(0)} \left|\psi'\right\rangle \otimes \left|j\right\rangle^{\otimes N} \tag{4.28}
$$

$$
\begin{aligned}
&= \frac{1}{c_0} P_1^{(0)} \left|\psi'\right\rangle \otimes \sum_j c_j \left|j\right\rangle^{\otimes N} \\
&= \left|\text{junk}\right\rangle \otimes \left|\psi_s\right\rangle,
\end{aligned}
$$

where to get (4.28) we used condition (4.23). It is an easy check to see that the whole proof above can be repeated by starting from a mixed joint state, yielding a corresponding version of the Lemma that holds for a general mixed state. □

We now describe the self-testing correlations for $\left|\psi_s\right\rangle = \sum_{j=0}^{d-1} c_j \left|j\right\rangle^{\otimes n}$. Their structure is inspired by the self-testing correlations from [CGS17] for the bipartite case, and they consist of three d-outcome measurements for all but the last party, which has four. We desribe them by first presenting the ideal measurements that achieve them, as we believe this aids understading. Subsequently, we extract their essential properties that guarantee self-testing. For a single-qubit observable A, denote by $[A]_m$ the observable defined with respect to the basis $\{\left|2m \mod d\right\rangle, \left|(2m+1) \mod d\right\rangle\}$. For example, $[\sigma_Z]_m = \left|2m\right\rangle\left\langle 2m\right| - \left|2m+1\right\rangle\left\langle 2m+1\right|$. Similarly, we denote by $[A]'_m$ the observable defined with respect to the basis $\{\left|(2m+1) \mod d\right\rangle, \left|(2m+2) \mod d\right\rangle\}$. We use the notation $\bigoplus A_i$ to denote the direct sum of observables A_i.

Let $\mathscr{X}_i$ denote the question set of the i-th party, and let $\mathscr{X}_i = \{0,1,2\}$ for $i = 1,\dots,N-1$, and $\mathscr{X}_N = \{0,1,2,3\}$. Let $x_i \in \mathscr{X}_i$ denote a question to the i-th party. The answer sets are $\mathscr{A}_i = \{0,1,\dots,d-1\}$, for $i = 1,\dots,N$.

Definition 5.1 (Ideal measurements for multipartite entangled Schmidt states)**.** *The N parties make the following measurements on the joint state $\left|\psi_s\right\rangle = \sum_{j=0}^{d-1} c_j \left|j\right\rangle^{\otimes n}$.*

For** $i = 1,\dots,N-1$**:

- *For question $x_i = 0$, the i-th party measures in the basis $\{\left|0\right\rangle, \left|1\right\rangle, \cdots, \left|d-1\right\rangle\}$,*

- *For* $x_i = 1$ *and* $x_i = 2$*: for d even, in the eigenbases of observables* $\bigoplus_{m=0}^{\frac{d}{2}-1}[\sigma_X]_m$ *and* $\bigoplus_{m=0}^{\frac{d}{2}-1}[\sigma_X]'_m$ *respectively, with the natural assignments of d measurement outcomes; for d odd, in the eigenbases of observables* $\bigoplus_{m=0}^{\frac{d-1}{2}-1}[\sigma_X]_m \oplus |d-1\rangle\langle d-1|$ *and* $|0\rangle\langle 0| \oplus \bigoplus_{m=0}^{\frac{d-1}{2}-1}[\sigma_X]'_m$ *respectively.*

For $i = N$*:*

- *For* $x_N = 0$ *and* $x_N = 1$*, the party N measures in the eigenbases of* $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu_m)\sigma_Z + \sin(\mu_m)\sigma_X]_m$ *and* $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu_m)\sigma_Z - \sin(\mu_m)\sigma_X]_m$ *respectively, with the natural assignments of d measurement outcomes, where* $\mu_m = \arctan[\sin(2\theta_m)]$ *and* $\theta_m = \arctan(c_{2m+1}/c_{2m})$*; for d odd, he measures in the eigenbases of* $\bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu_m)\sigma_Z + \sin(\mu_m)\sigma_X]_m \oplus |d-1\rangle\langle d-1|$ *and* $\bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu_m)\sigma_Z - \sin(\mu_m)\sigma_X]_m \oplus |d-1\rangle\langle d-1|$ *respectively.*

- *For* $x_N = 2$ *and* $x_N = 3$*: for d even, the N-th party measures in the eigenbases of* $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu'_m)\sigma_Z + \sin(\mu'_m)\sigma_X]'_m$ *and* $\bigoplus_{m=0}^{\frac{d}{2}-1}[\cos(\mu'_m)\sigma_Z - \sin(\mu'_m)\sigma_X]'_m$ *respectively, where* $\mu'_m = \arctan[\sin(2\theta'_m)]$ *and* $\theta'_m = \arctan(c_{2m+2}/c_{2m+1})$*; for d odd, in the eigenbases of* $|0\rangle\langle 0| \oplus \bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu'_m)\sigma_Z + \sin(\mu'_m)\sigma_X]'_m$ *and* $|0\rangle\langle 0| \oplus \bigoplus_{m=0}^{\frac{d-1}{2}-1}[\cos(\mu'_m)\sigma_Z - \sin(\mu'_m)\sigma_X]'_m$*, respectively.*

We refer to the correlation specified by the ideal measurements above as the ideal correlation for multipartite entangled Schmidt states.

Next, we will highlight a set of properties of the ideal correlation that are enough to characterize it, in the sense that any quantum correlation that satisfies these properties has to be the ideal one. This also aids understanding of the self-testing proof (Proof of Theorem 6). In what follows, we will employ the language of correlation tables, which gives a convenient way to describe correlations. In general, let $\mathscr{X}_i$ be the question sets and $\mathscr{A}_i$ the answer sets. A correlation specifies, for each possible question $x \in \mathscr{X}_1 \times \cdots \times \mathscr{X}_{\mathscr{N}}$, a table T_x with entries $T_x(a) = p(a|x)$ for $a \in \mathscr{A}_1 \times \cdots \times \mathscr{A}_N$. For example, we denote the correlation tables for the ideal correlations for multipartite entangled GHZ states from Theorem 5 as $T_x^{\mathrm{ghz}_N(\theta_m)}$, where $x \in \{0,1\}^N$ denotes the question.

Definition 5.2 (Self-testing properties of the ideal correlations for multipartite entangled Schmidt states)**.** *Recall that* $\mathscr{X}_i = \{0,1,2\}$ *for* $i = 1,\ldots,N-1$*, and* $\mathscr{X}_N = \{0,1,2,3\}$*.* $\mathscr{A}_i = \{0,1,\ldots,d-1\}$*, for* $i = 1,\ldots,N$*.*

The self-testing properties of the ideal correlations are:

- *For questions* $x \in \{0,1\}^N$*, we require* T_x *to be block-diagonal with* 2^N *blocks* $C_{x,m} := (c_{2m}^2 + c_{2m+1}^2) \cdot T_x^{ghz_N(\theta_m)}$ *corresponding to outcomes in* $\{2m, 2m+1\}^N$*, where the multiplication by the weight is intended entry-wise, and* $\theta_m := \arctan\left(\frac{c_{2m+1}}{c_{2m}}\right)$*.*

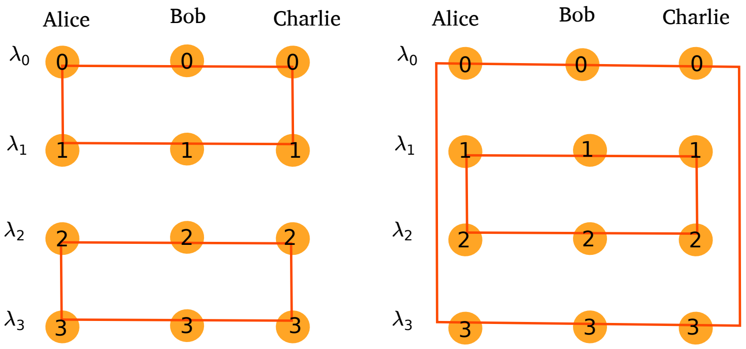

Figure 4.3: A sketch of the self-testing protocol of the tripartite ququart Schmidt state $\lambda_0 |000\rangle + \lambda_1 |111\rangle + \lambda_2 |222\rangle + \lambda_3 |333\rangle$. The balls represent different degrees of freedom and solid lines denote which degrees of freedom are entangled. The left part corresponds to the situation when Alice, Bob and Charlie get inputs 0 or 1. The ideal measurements can be used to self-test subnormalized states $\lambda_0 |00\rangle + \lambda_1 |11\rangle$ and $\lambda_2 |22\rangle + \lambda_3 |33\rangle$. The right part corresponds to the situation when Alice and Bob get inputs 0 and 2 and Charlie gets inputs 2 and 3. The ideal measurements can be used to self-test subnormalized states $\lambda_0 |00\rangle + \lambda_3 |33\rangle$ and $\lambda_2 |11\rangle + \lambda_3 |22\rangle$. These two sub-tests, when merged, are enough to self-test the full state.

- *For questions with $x_i \in \{0,2\}$, for $i = 1,\dots,N-1$ and $x_N \in \{2,3\}$ we require T_x to be block-diagonal with the $2^{\times N}$ blocks ”shifted down” by one measurement outcome. These should be $D_{x,m} := (c_{2m+1}^2 + c_{2m+2}^2) \cdot T^{ghz_N(\theta'_m)}_{f(x_1),\dots,f(x_{N-1}),g(x_N)}$ corresponding to measurement outcomes in $\{2m+1, 2m+2\}^N$, where $\theta'_m := \arctan\left(\frac{c_{2m+2}}{c_{2m+1}}\right)$ and $f(0) = 0$, $f(2) = 1$, $g(2) = 0$, $g(3) = 1$.*

We are now ready to state the main theorem of this section.

Theorem 6. *Suppose N parties exhibit the ideal correlations for multipartite entangled Schmidt states from Definition 5.1 by making local measurements on a joint state $|\psi'\rangle$. Then there exists a local isometry Φ such that $\Phi(|\psi'\rangle) = |\text{junk}\rangle \otimes |\psi_s\rangle$.*

Proof. We work in the tripartite case, as the general n-partite case follows analogously. The measurements of Alice, Bob and Charlie can be assumed to be projective, since we make no assumption on the dimension of the system. For ease of notation, the proof assumes that the joint state is pure, but one easily realizes that the proof goes through in the same way by rephrasing everything in terms of density matrices (see Ref. [CGS17] for a slightly more detailed discussion).

Let $P^a_{A_x}$ be the projection on Alice side corresponding obtaining outcome a on question x. Analogously, define $P^b_{B_y}$ and $P^c_{C_z}$ on Bob and Charlie's side, respectively. The proof structure follows closely that of [CGS17], and goes through explicitly constructing projectors and unitary operators satisfying the sufficient conditions of Lemma 5.1.

Define $\hat{A}_{x,m} = P^{2m}_{A_x} - P^{2m+1}_{A_x}$, $\hat{B}_{y,m} = P^{2m}_{B_y} - P^{2m+1}_{B_y}$ and $\hat{C}_{z,m} = P^{2m}_{C_z} - P^{2m+1}_{C_z}$, for $x,y,z \in \{0,1\}$. Let $\mathbb{1}^m_{A_x} = P^{2m}_{A_x} + P^{2m+1}_{A_x}$ and similarly define $\mathbb{1}^m_{B_y}$ and $\mathbb{1}^m_{C_z}$ for $x,y,z \in \{0,1\}$. Now,

$$\begin{aligned} \|P^{2m}_{A_0}\| &= \sqrt{\langle\psi'|P^{2m}_{A_0}|\psi'\rangle} \\ &= \sqrt{\langle\psi'|P^{2m}_{A_0}\sum_{i=0}^{d-1}P^i_{B_0}\sum_{j=0}^{d-1}P^j_{C_0}|\psi'\rangle} \\ &= c_{2m}, \end{aligned} \tag{4.29}$$

and $\|P^{2m+1}_{A_0}\| = c_{2m+1}$. Similarly, we derive $\|\mathbb{1}^m_{A_x}|\psi'\rangle\| = \|\mathbb{1}^m_{B_y}|\psi'\rangle\| = \|\mathbb{1}^m_{C_z}|\psi'\rangle\| = (c^2_{2m} + c^2_{2m+1})^{1/2}$ for any m and $x,y,z \in \{0,1\}$. Notice then that

$$\begin{aligned} \langle\psi'|\mathbb{1}^m_{A_x}\mathbb{1}^m_{B_y}|\psi'\rangle &= \langle\psi'|\mathbb{1}^m_{A_x}\mathbb{1}^m_{B_y}\sum_{i=0}^{d-1}P^i_{C_0}|\psi'\rangle \\ &= \langle\psi'|\mathbb{1}^m_{A_x}\mathbb{1}^m_{B_y}\mathbb{1}^m_{C_0}|\psi'\rangle \\ &= c^2_{2m} + c^2_{2m+1}, \end{aligned} \tag{4.30}$$

where the second last equality is from the block-diagonal structure of the correlations. Since $\|\mathbb{1}^m_{A_x}|\psi'\rangle\| = \|\mathbb{1}^m_{B_y}|\psi'\rangle\| = (c^2_{2m} + c^2_{2m+1})^{1/2}$, then Cauchy-Schwartz inequality implies $\mathbb{1}^m_{A_x}|\psi'\rangle = \mathbb{1}^m_{B_y}|\psi'\rangle$. So, we have

$$\mathbb{1}^m_{A_x}|\psi'\rangle = \mathbb{1}^m_{B_y}|\psi'\rangle = \mathbb{1}^m_{C_z}|\psi'\rangle \tag{4.31}$$

for all $x,y,z \in \{0,1\}$. The correlations are, by design, such that $\hat{A}_{0,m}, \hat{A}_{1,m}, \hat{B}_{0,m}, \hat{B}_{1,m}, \hat{C}_{0,m}$, $\hat{C}_{1,m}$, the associated projections $P^j_{A_i}, P^j_{B_i}, P^j_{C_i}$, $j \in \{2m, 2m+1\}$ and $|\psi'\rangle$ reproduce the correlations $(c^2_{2m} + c^2_{2m+1}) \cdot C^{\mathrm{ghz}_{3,2,\theta_m}}_{x,y,z}$. In order to apply Theorem 5, we need to define the normalized state $|\psi'_m\rangle := (\mathbb{1}^m_{A_0}|\psi'\rangle)/(c^2_{2m} + c^2_{2m+1})^{1/2}$ and the "unitarized" versions of the operators above, namely $\hat{D}_{i,m} := \mathbb{1} - \mathbb{1}^{D_i}_m + \hat{D}_{i,m}$, for $D \in \{A,B,C\}$. It is easy to check that then $\hat{A}_{i,m}, \hat{B}_{i,m}$ and $\hat{C}_{i,m}$ satisfy the conditions of Theorem 5 (for $N = 3$) on state $|\psi'_m\rangle$. Thus, we have

$$Z_{A,m}|\psi'_m\rangle = Z_{B,m}|\psi'_m\rangle = Z_{C,m}|\psi'_m\rangle, \tag{4.32}$$

$$X_{A,m}X_{B,m}X_{C,m}(\mathbb{1} - Z_{A,m})|\psi'_m\rangle = \tan(\theta_m)(\mathbb{1} + Z_{A,m})|\psi'_m\rangle. \tag{4.33}$$

Define the subspace $\mathscr{C}_m = \mathrm{range}(\mathbb{1}^{C_0}_m) + \mathrm{range}(\mathbb{1}^{C_1}_m)$, and the projection $\mathbb{1}_{\mathscr{C}_m}$ onto subspace $\mathscr{C}_m$. Then, notice from the way $Z_{C,m}$ is defined, that it can be written as $Z_{C,m} = \mathbb{1} - \mathbb{1}_{\mathscr{C}_m} + \tilde{Z}_{C,m}$, where $\tilde{Z}_{C,m}$ is some operator living entirely on subspace $\mathscr{C}_m$. This implies that $Z_{C,m}|\psi'_m\rangle = \tilde{Z}_{C,m}|\psi'_m\rangle = \tilde{Z}_{C,m}|\psi'\rangle$, where we have used Eq. (4.31) and the fact that

$$\mathbb{1}^{C_0}_m|\psi'\rangle = \mathbb{1}^{C_1}_m|\psi'\rangle \implies \mathbb{1}_{\mathscr{C}_m}|\psi'\rangle = \mathbb{1}^{C_i}_m|\psi'\rangle\,. \tag{4.34}$$

Hence, from Eq. (4.32) it is not difficult to deduce that $\hat{A}_{0,m}|\psi'\rangle = \hat{B}_{0,m}|\psi'\rangle = \tilde{Z}_{C,m}|\psi'\rangle$.

Constructing the projections of Lemma 5.1. Define projections $P_A^{(2m)} := (\mathbb{1}_m^{A_0} + \hat{A}_{0,m})/2 = P_{A_0}^{2m}$, $P_A^{(2m+1)} := (\mathbb{1}_m^{A_0} - \hat{A}_{0,m})/2 = P_{A_0}^{2m+1}$, $P_B^{(2m)} := (\mathbb{1}_m^{B_0} + \hat{B}_{0,m})/2 = P_{B_0}^{2m}$, $P_B^{(2m+1)} := (\mathbb{1}_m^{B_0} - \hat{B}_{0,m})/2 = P_{B_0}^{2m+1}$, $P_C^{(2m)} := (\mathbb{1}_{\mathscr{C}_m} + \tilde{Z}_{C,m})/2$ and $P_C^{(2m+1)} := (\mathbb{1}_{\mathscr{C}_m} - \tilde{Z}_{C,m})/2$.

Note that $P_C^{(2m)}, P_C^{(2m+1)}$ are indeed projections, since $\tilde{Z}_{C,m}$ has all ± 1 eigenvalues corresponding to subspace $\mathscr{C}_m$, and is zero outside. We also have, for all m and $k = 2m, 2m+1$,

$$\begin{aligned} P_B^{(k)}|\psi\rangle = P_A^{(k)}|\psi'\rangle = \frac{1}{2}[\mathbb{1}_m^{A_0} + (-1)^k \hat{A}_{0,m}]|\psi'\rangle &= \frac{1}{2}[\mathbb{1}_m^{B_0} + (-1)^k \hat{A}_{0,m}]|\psi'\rangle \\ &= \frac{1}{2}[\mathbb{1}_{\mathscr{B}_m} + (-1)^k \tilde{Z}_{B,m}]|\psi'\rangle = P_C^{(k)}|\psi'\rangle. \end{aligned} \tag{4.35}$$

Further, notice that

$$[\mathbb{1} + (-1)^k Z_{A,m}]|\psi'_m\rangle = [\mathbb{1}_m^{A_0} + (-1)^k \hat{A}_{0,m}]|\psi'_m\rangle = [\mathbb{1}_m^{A_0} + (-1)^k \hat{A}_{0,m}]|\psi'\rangle = P_A^{(k)}|\psi'\rangle.$$

Substituting this into (4.33), gives

$$X_{A,m}X_{B,m}X_{C,m}P_A^{(2m+1)}|\psi'\rangle = \tan(\theta_m)P_A^{(2m)}|\psi'\rangle = \frac{c_{2m+1}}{c_{2m}}P_A^{(2m)}|\psi'\rangle. \tag{4.36}$$

Now, for the "shifted" blocks, we can similarly define $\hat{A}'_{x,m}$, $\hat{B}'_{x,m}$ and $\hat{C}'_{x,m}$ as $\hat{A}_{x,m} = P_{A_x}^{2m+1} - P_{A_x}^{2m+2}$ and similar. Then, analogously, we deduce the existence of hermitian and unitary operators $Y'_{A,m}$, $Y'_{B,m}$ and $Y'_{C,m}$ such that

$$Y_{A,m}Y_{B,m}Y_{C,m}P_A^{(2m+2)}|\psi'\rangle = \frac{c_{2m+2}}{c_{2m+1}}P_A^{(2m+1)}|\psi'\rangle. \tag{4.37}$$

Constructing the unitary operators of Lemma 5.1. We will now directly construct unitary operators satisfying conditions (4.23,4.24) of Lemma 5.1. Define $X_{A/B/C}^{(k)}$ as follows:

$$X_A^{(k)} = \begin{cases} \mathbb{1}, & \text{if } k = 0, \\ X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\ldots X_{A,m-1}Y_{A,m-1}X_{A,m}, & \text{if } k = 2m+1, \\ X_{A,0}Y_{A,0}X_{A,1}Y_{A,1}\ldots X_{A,m-1}Y_{A,m-1}, & \text{if } k = 2m, \end{cases} \tag{4.38}$$

and analogously for $X_B^{(k)}$ and $X_C^{(k)}$. Note that $X_A^{(k)}$ and $X_B^{(k)}$ are unitary since they are product of unitaries. Finally, we are left to check that

$$X_A^{(k)}X_B^{(k)}X_C^{(k)}P_A^{(k)}|\psi'\rangle = \frac{c_k}{c_0}P_A^{(0)}|\psi'\rangle. \tag{4.39}$$

The case $k=0$ holds trivially. For $k=2m+1$, For $k=2m+1$,

$$\begin{aligned}
&X_A^{(k)}X_B^{(k)}X_C^{(k)}P_A^{(k)}\,|\psi'\rangle \\
&\qquad = X_{A,0}Y_{A,0}X_{B,0}Y_{B,0}X_{C,0}Y_{C,0}\dots X_{A,m-1}Y_{A,m-1}X_{B,m-1}Y_{B,m-1}X_{C,m-1}Y_{C,m-1} \\
&\qquad\quad \times X_{A,m}X_{B,m}X_{C,m}P_A^{(2m+1)}\,|\psi'\rangle \\
&\qquad \overset{(4.36)}{=} \frac{c_{2m+1}}{c_{2m}}X_{A,0}Y_{A,0}X_{B,0}Y_{B,0}X_{C,0}Y_{C,0}\dots X_{A,m-1}Y_{A,m-1}X_{B,m-1}Y_{B,m-1}X_{C,m-1}Y_{C,m-1}P_A^{(2m)}\,|\psi'\rangle \\
&\qquad \overset{(4.37)}{=} \frac{c_{2m+1}}{c_{2m}}\cdot\frac{c_{2m}}{c_{2m-1}}X_{A,0}Y_{A,0}X_{B,0}Y_{B,0}X_{C,0}Y_{C,0}\dots X_{A,m-2}Y_{A,m-2}X_{B,m-2}Y_{B,m-2} \\
&\qquad\quad \times X_{C,m-2}Y_{C,m-2}P_A^{(2m-1)}\,|\psi'\rangle \\
&\qquad = \dots \\
&\qquad = \frac{c_{2m+1}}{\cancel{c_{2m}}}\cdot\frac{\cancel{c_{2m}}}{\cancel{c_{2m-1}}}\cdots\frac{\cancel{c_2}}{\cancel{c_1}}\cdot\frac{\cancel{c_1}}{c_0}P_A^{(0)}\,|\psi'\rangle \\
&\qquad = \frac{c_{2m+1}}{c_0}P_A^{(0)}\,|\psi'\rangle
\end{aligned} \tag{4.40}$$

which is indeed (4.39) as $2m+1=k$. The case $k=2m$ is similar. This concludes the proof of Theorem 6. □

4.3 Self-testing W-state

In this section we provide a detailed proof of self-testing of the $|W_N\rangle$ state

$$|W_N\rangle = \frac{1}{\sqrt{N}}(|0\dots01\rangle + |0\dots010\rangle + \dots + |10\dots0\rangle). \tag{4.41}$$

For the sake of proof simplicity we show how to self-test the following unitarily equivalent state

$$|xW_N\rangle = \frac{1}{\sqrt{N}}(|0\dots0\rangle + |0\dots011\rangle + \dots + |10\dots01\rangle). \tag{4.42}$$

which is obtained from $|W_N\rangle$ by applying σ_X to the last qubit of $|W_N\rangle$. This is because $|xW_N\rangle$ can be written as

$$|xW_N\rangle = \frac{1}{\sqrt{N}}\left[|0\rangle^{\otimes N-2}(|00\rangle+|11\rangle)_{i,N} + |\text{rest}_i\rangle\right], \tag{4.43}$$

where $(|00\rangle+|11\rangle)_{i,N}$ stands for the two-qubit maximally entangled state distributed between the parties i and N with $i=1,\dots,N-1$, and the vectors $|\text{rest}_i\rangle$ contain the remaining kets. This decomposition explains the conditions we impose below.

Let us now prove the following theorem.

Theorem 7. *Assume that for a given state $|\psi'\rangle$ and measurements Z_i, X_i for parties $i = 1,\ldots,N-1$ and D_N and E_N for the last party, the following conditions are satisfied*

$$\left\langle \bigotimes_{\substack{l=1\\l\neq i}}^{N-1} Z_l^{(+)} \right\rangle = \frac{2}{N}, \qquad \left\langle \bigotimes_{\substack{l=1\\l\neq i}}^{N-1} Z_l^{(+)} \otimes \mathscr{B}_{i,N}^{(+)} \right\rangle = \frac{4\sqrt{2}}{N}, \tag{4.44}$$

with $i = 1,\ldots,N-1$, where, $\mathscr{B}_{i,N}^{(+)}$ is the Bell operator between the parties i and N corresponding to the CHSH Bell inequality

$$\mathscr{B}_{i,N}^{(+)} = Z_i \otimes D_N + Z_i \otimes E_N + X_i \otimes D_N - X_i \otimes E_N. \tag{4.45}$$

Moreover, we assume that

$$\langle Z_i^{(-)} \rangle = \frac{1}{N}, \qquad \left\langle \bigotimes_{\substack{l=1\\l\neq i}}^{N-1} Z_i^{(+)} \otimes Z_i^{(-)} \right\rangle = \frac{1}{N} \tag{4.46}$$

with $i = 1,\ldots,N-1$. Then, for the isometry Φ_N one has

$$\Phi_N\left(|\psi'\rangle\,|0\rangle^{\otimes N}\right) = |\mathrm{junk}\rangle\,|xW_N\rangle\,. \tag{4.47}$$

Before giving the detailed proof, let us present here the main idea. The proof makes use of the fact that $|xW_N\rangle$ can be written as $[|0\rangle^{\otimes N-2}(|00\rangle + |11\rangle)_{i,N} + |\mathrm{rest}_i\rangle]/\sqrt{N}$, where $(|00\rangle + |11\rangle)_{i,N}$ is the maximally entangled state between the parties i and N, and the state $|\mathrm{rest}_i\rangle$ collects all the remaining kets. We thus impose in Eq. (**??**) that if $(N-2)$-partite subset of the first $N-1$ parties obtains $+1$ when measuring Z_i on $|\psi'\rangle$, the state held by the parties i and N violates maximally the CHSH Bell inequality. Conditions in (**??**) are needed to characterize $|\mathrm{rest}_i\rangle$, which completes the proof.

Proof. Denoting $Z_N = (D_N + E_N)/\sqrt{2}$ and $X_N = (D_N - E_N)/\sqrt{2}$, the action of the isometry can be explicitly written as

$$\Phi_N\left(|\psi'\rangle\,|0\rangle^{\otimes N}\right) = \sum_{\tau\in\{0,1\}^N} X_1^{\tau_1}\ldots X_N^{\tau_N} Z_1^{(\tau_1)}\ldots Z_N^{(\tau_N)}\,|\psi'\rangle\,|\tau_1\ldots\tau_N\rangle\,, \tag{4.48}$$

where $\tau = (\tau_1,\ldots,\tau_N)$ with each $\tau_i \in \{0,1\}$ and $Z_i^{(\tau_i)} = [\mathbb{1} + (-1)^{\tau_i} Z_i]/2$.

It should be noticed that in general the operators Z_N and D_N might not be unitary, and one should consider $\widetilde{X}_N$ and $\widetilde{Z}_N$, which by constructions are unitary. However, following the regularization procedure, explained in Chapter 3, their action on $|\psi'\rangle$ is the same as the action of X_N and Z_N, thus, for simplicity, we use these operators.

The first bunch of conditions (4.44) implies that the norm of

$$|\psi_i\rangle = Z_1^{(+)}\ldots Z_{i-1}^{(+)} Z_{i+1}^{(+)}\ldots Z_{N-1}^{(+)}\,|\psi'\rangle \tag{4.49}$$

is $\sqrt{2/N}$, which together with the second set of conditions in Eq. (4.44) implies that the normalized states $|\widetilde{\psi}_i\rangle = \sqrt{N/2}\,|\psi_i\rangle$ violate maximally the CHSH Bell inequality between the parties i and N for $i = 1,\ldots,N-1$. This, by virtue of Lemma 4.1, yields the following identities

$$(Z_i - Z_N)\,|\widetilde{\psi}_i\rangle = 0 \tag{4.50}$$
$$[X_i(I+Z_N) - X_N(I-Z_i)]\,|\widetilde{\psi}_i\rangle = 0 \tag{4.51}$$
$$\{Z_i, X_i\}\,|\widetilde{\psi}_i\rangle = 0. \tag{4.52}$$

They immediately imply that all terms in Eq. (4.48) for which one element of τ equals one and the rest equal zero vanish. To see it explicitly, let $\tau_i = 1$ and $\tau_j = 0$ for $j \neq i$. Then, for this τ, $|\psi_\tau\rangle = X_i Z_i^{(-)} Z_N^{(+)}\,|\psi_i\rangle$. Applying (4.50) to the latter and exploiting the fact that $Z_i^{(-)} Z_i^{(+)} = 0$, one finally finds that $|\psi_\tau\rangle = 0$.

Let us now consider those components of Eq. (4.48) for which τ obeys $\tau_i = \tau_N = 1$ with $i = 1,\ldots,N-1$ and $\tau_j = 0$ with $j \neq i,N$. Then, the following chain of equalities holds

$$\begin{aligned}
Z_1^{(+)} \ldots Z_{i-1}^{(+)} X_i Z_i^{(-)} Z_{i+1}^{(+)} \ldots Z_{N-1}^{(+)} X_N Z_N^{(-)}\,|\psi'\rangle &= X_i Z_i^{(-)} X_N Z_N^{(-)}\,|\psi_i\rangle \\
&= X_i Z_i^{(-)} X_N Z_i^{(-)}\,|\psi_i\rangle \\
&= X_i Z_i^{(-)} X_i Z_N^{(+)}\,|\psi_i\rangle \\
&= Z_i^{(+)} Z_N^{(+)}\,|\psi_i\rangle \\
&= Z_1^{(+)} \ldots Z_N^{(+)}\,|\psi'\rangle,
\end{aligned} \tag{4.53}$$

where the second equality stems from Eq. (4.50), the third from Eq. (4.51), and, finally, the fourth equality is a consequence of the anticommutation relation (4.52) and the fact that $X_i^2 = \mathbb{1}$.

With all this in mind it is possible to group the terms in Eq. (4.48) in the following way

$$\Phi_N(|\psi'\rangle\,|0\rangle^{\otimes N}) = |\text{junk}\rangle\,|xW_N\rangle + |\Omega\rangle, \tag{4.54}$$

where $|\text{junk}\rangle = \sqrt{N} Z_1^{(+)} \ldots Z_N^{(+)}\,|\psi\rangle$ and $|\Omega\rangle$ contains all those terms for which τ contains more than two ones or exactly two ones but $\tau_N = 0$.

Now, our aim is to prove that $|\Omega\rangle = 0$. To this end we first notice that Eqs. (4.46) imply the following correlations

$$\langle\psi'|Z_i^{(-)} Z_j^{(+)}|\psi'\rangle = \frac{1}{N}, \tag{4.55}$$

where $i \neq j$ and $i,j = 1,\ldots,N-1$. This is a direct consequence of the fact that $Z_i^{(\pm)} \leq \mathbb{1}$, which in turn implies that each of correlators in (4.55) is bounded from above by

$\langle\psi'|Z_i^{(-)}|\psi'\rangle$ and from below by $\langle\psi'|Z_1^{(+)}\ldots Z_{i-1}^{(+)}Z_i^{(-)}Z_{i+1}^{(+)}\ldots Z_{N-2}^{(+)}Z_{N-1}^{(+)}|\psi'\rangle$ and both are assumed to equal $1/N$ [cf. Eq. (4.46)].

The first relation in Eq. (4.55) together with Eq. (4.46) and the fact that $Z_j^{(+)}+Z_j^{(-)}=\mathbb{1}$ yields $\langle\psi'|Z_i^{(-)}Z_j^{(-)}|\psi'\rangle=0$. This, due to the fact that $Z_i^{(-)}Z_j^{(-)}$ is a projector, allows one to write

$$Z_i^{(-)}Z_j^{(-)}|\psi'\rangle=0 \tag{4.56}$$

for $i,j=1,\ldots,N-1$. This is enough to conclude that $|\Omega\rangle=0$, which when plugged into Eq. (4.43), leads directly to Eq. (4.47) because each component in $|\Omega\rangle$ has either three τ_i which equal 1, or two τ_i that equal one but then $\tau_N=0$.

Since the self-test relies on the maximal violation of the CHSH Bell inequality by a set of states $|\widetilde{\psi}_i\rangle$ $(i=1,\ldots,N-1)$, it also inherits self-testing of the optimal CHSH measurements, meaning that

$$\begin{aligned}\Phi_N\left(Z_i|\psi'\rangle|0\rangle^{\otimes N}\right)&=|\text{junk}\rangle\otimes\sigma_{\text{Z}}^{(i)}|xW_N\rangle\\ \Phi_N\left(X_i|\psi'\rangle|0\rangle^{\otimes N}\right)&=|\text{junk}\rangle\otimes\sigma_{\text{X}}^{(i)}|xW_N\rangle\end{aligned} \tag{4.57}$$

for $i=1,\ldots,N-1$, and

$$\begin{aligned}\Phi_N\left(D_N|\psi'\rangle|0\rangle^{\otimes N}\right)&=|\text{junk}\rangle\otimes\frac{\sigma_{\text{Z}}^{(i)}+\sigma_{\text{X}}^{(i)}}{\sqrt{2}}|xW_N\rangle,\\ \Phi_N\left(E_N|\psi'\rangle|0\rangle^{\otimes N}\right)&=|\text{junk}\rangle\otimes\frac{\sigma_{\text{Z}}^{(i)}-\sigma_{\text{X}}^{(i)}}{\sqrt{2}}|xW_N\rangle.\end{aligned} \tag{4.58}$$

This completes the proof. □

It should be noticed that our self-test of the W state exploits two observables per site and, as in the case of the partially entangled GHZ state, the number of correlators one needs to determine is $2N$, and thus scales linearly with N.

4.4 Symmetric Dicke states

Let us now consider the symmetric Dicke states. These are simultaneous eigenstates of the square of the total angular momentum operator $\mathbf{J}^2$ of N qubits and its projection onto the z-axis J_z. In a concise way they can be stated as

$$|D_N^k\rangle=\frac{1}{\sqrt{\binom{N}{k}}}\sum_i P_i(|1\rangle^{\otimes k}|0\rangle^{\otimes(N-k)}), \tag{4.59}$$

where the sum goes over all permutations of the parties and k is the number of excitations. For instance, for $k=1$ they reproduce the N-qubit W state:

$$|W_N\rangle=\frac{1}{\sqrt{N}}(|0\ldots01\rangle+|0\ldots10\rangle+\ldots+|10\ldots0\rangle). \tag{4.60}$$

Interestingly, Dicke states have been generated experimentally [Pre+09] and have important role in metrology tasks [Kri+11] and quantum networking protocols [Chi+12].

Let us now show how the self-test of the N-partite W state can be used to construct a self-test of all the Dicke states. Notice that a Dicke state with $m \leq \lfloor N/2 \rfloor$ is unitarily equivalent to a Dicke state with $m \geq \lceil N/2 \rceil$, i.e., $|D_N^m\rangle = \sigma_Z^{\otimes N} |D_N^{N-m}\rangle$ for $m = 0, \ldots, \lfloor N/2 \rfloor$. For this reason below we consider the Dicke states with $m \geq \lfloor N/2 \rfloor$. To facilitate our considerations we show how to self-test the following unitarlity equivalent state

$$\begin{aligned} |xD_N^m\rangle &= \sigma_Z^{(N)} |xD_N^m\rangle \\ &= \sum_{i_1,\ldots,i_{N-m-1}=0}^{1} \frac{\sqrt{\binom{m+1}{m-\Sigma}}}{\sqrt{\binom{N}{m}}} |i_1, \ldots, i_{N-m-1}\rangle |xD_{m+1}^{m-\Sigma}\rangle . \end{aligned} \tag{4.61}$$

We then notice that the state corresponding to $i_1 = \ldots = i_{N-m-1} = 0$ is exactly $|xD_{m+1}^m\rangle = \sigma_X^{\otimes(m+1)} |xW_{m+1}\rangle$ with $|xW_{m+1}\rangle$ defined in Eq.(4.41). Moreover, since $|xD_N^m\rangle$ is symmetric on the first $N-1$ parties, the state $\sigma_X^{\otimes(m+1)} |xW_{m+1}\rangle$ will appear in any decomposition of the form (4.61) in which any choice of $N-m-1$ parties from the first $N-1$ ones are in state $|0\rangle$. Importantly, we already know how to self-test the W state $\sigma_X^{\otimes(m+1)} |xW_{m+1}\rangle$. However, due to the transformation $\sigma_X^{\otimes(m+1)}$ we have to modify the conditions specified in Theorem 7 in the following way:

$$\begin{aligned} &Z_i^{(+)} \leftrightarrow Z_i^{(-)} \quad (i = 1, \ldots, N-1), \\ &D_N \rightarrow -E_N \quad \text{and} \quad E_N \rightarrow -D_N. \end{aligned} \tag{4.62}$$

Now, to self-test a Dicke state $|D_N^m\rangle$ for any $m \geq \lfloor N/2 \rfloor$ we can proceed in the following way:

1. Project any $(N-m-1)$-element subset $\mathscr{S}_i$ of the first $N-1$ parties of $|\psi\rangle$ (there are $\binom{N-1}{N-1-m}$ such subsets) onto $\bigotimes_{j \in \mathscr{S}_i} Z_j^{(+)}$ and check whether the state corresponding to the remaining parties satisfies the conditions for $|xD_{m+1}^m\rangle = \sigma_X^{\otimes(m+1)} |xW_{m+1}\rangle$.

2. For every sequence $\tau = (\tau_1, \ldots, \tau_N)$ consisting of $m+1$ ones on the first $N-1$ positions, check that the state $|\psi\rangle$ obeys the following correlations

$$\langle \psi' | Z_1^{(\tau_1)} \otimes \ldots \otimes Z_N^{(\tau_N)} | \psi' \rangle = 0, \tag{4.63}$$

where $Z_i^{(\tau_i)} = [\mathbb{1} + (-1)^{\tau_i} Z_i]/2$

Let us now see in more details how the above procedure allows one to self-test $|D_N^m\rangle$. It is not difficult to see that the first condition leads us to the following decomposition

$$\Phi_N(|\psi'\rangle\,|0\rangle^{\otimes N}) = \left[\bigotimes_{l\in\mathscr{S}_i} Z_l^{(+)}\,|\text{junk}_i\rangle\right]\otimes\left[|0\rangle_{\mathscr{S}_i}^{\otimes(N-m-1)}\,|xD_{m+1}^m\rangle\right]+|\Phi_i\rangle \tag{4.64}$$

for any $i=1,\ldots,\binom{N-1}{N-1-m}$, where all $\mathscr{S}_i$ stand for different $(N-m-1)$-element subsets of the $(N-1)$-element set $\{1,\ldots,N-1\}$, and $|\text{junk}_i\rangle$ is defined as

$$|\text{junk}_i\rangle = \bigotimes_{l\in\{1,\ldots,N\}\setminus\mathscr{S}_i} X_l Z_l^{(-)}\,|\psi'\rangle\,. \tag{4.65}$$

In other words, to construct $|\text{junk}_i\rangle$ from $|\psi'\rangle$ one has to act on the latter with $X_l Z_l^{(-)}$ on all parties who do not belong to $\mathscr{S}_i$. Finally, $|\Phi_i\rangle$ is some state from the global Hilbert space collecting the remaining terms.

Let us now show that all the states

$$|\text{junk}_i'\rangle = \bigotimes_{l\in\mathscr{S}_i} Z_l^{(+)}\,|\text{junk}_i\rangle \tag{4.66}$$

are the same. To this end, we will exploit the conditions (4.50) and (4.52), which are clearly preserved under the transformation (4.62), and also the fact that:

$$(X_i - X_N)\,|\psi'\rangle = |\psi'\rangle \tag{4.67}$$

for any $i=1,\ldots,N-1$. Consider two vectors $|\text{junk}_i'\rangle$ and $|\text{junk}_j'\rangle$ such that the corresponding sets $\mathscr{S}_i$ and $\mathscr{S}_j$ share $N-m-2$ elements (remember that these sets are equinumerous). Let q and p be the two elements by which these sets differ, i.e., $p\in\mathscr{S}_i$ ($q\in\mathscr{S}_j$) and $p\notin\mathscr{S}_j$ ($q\notin\mathscr{S}_i$). Then, using the condition (4.52) we turn the operator $X_t Z_t^{(-)}$ into $Z_t^{(+)}X_t$ at positions $t=q$ and $t=N$ for the state $|\text{junk}_i'\rangle$, and, analogously, at positions $t=p$ and $t=N$ for the state $|\text{junk}_j'\rangle$. We utilize the fact that $X_i X_N\,|\psi'\rangle = |\psi'\rangle$ for all $i=1,\ldots,N-1$ stemming from (4.67), which shows that $|\text{junk}_i'\rangle = |\text{junk}_j'\rangle$. Finally, repeating this procedure for all pairs of states for which the corresponding sets $\mathscr{S}_i$ differ by two elements, one finds that $|\text{junk}_i'\rangle \equiv |\text{junk}\rangle$ for all i.

As a result, the state (4.64) simplifies to

$$\Phi_N(|\psi'\rangle\,|0\rangle^{\otimes N}) = |\text{junk}\rangle\,|xD_N^m\rangle + |\Phi\rangle\,, \tag{4.68}$$

$|\Phi\rangle$ is a vector from the global Hilbert space defined as

$$|\Phi\rangle = \sum_{\tau}\left(X_1^{\tau_1}Z_1^{(\tau_1)}\otimes\ldots\otimes X_N^{\tau_N}Z_N^{(\tau_N)}\,|\psi'\rangle\right)\otimes|\tau\rangle\,, \tag{4.69}$$

where the summation is over all sequences $\tau = (\tau_1, \ldots, \tau_N)$ that contain less than $N - m - 1$ zeros (or, equivalently, more than m ones) on the first $N - 1$ positions.

Now, to prove that $|\Phi\rangle = 0$ it suffices to exploit the second step in the above procedure. That is, the condition (4.63) is equivalent to

$$Z_1^{(\tau_1)} \otimes \ldots \otimes Z_N^{(\tau_N)} |\psi'\rangle = 0 \tag{4.70}$$

for every sequence $(\tau_1, \ldots, \tau_N)$ consisting of $m+1$ ones at the first $N-1$ positions. Then, every component of the vector in Eq. (4.69) contains a sequence of at least $m+1$ $Z^{(-)}$ operators, which by virtue of (4.70) implies that $|\Phi\rangle = 0$. This completes the proof.

For the self-testing of measurements the same argumentation as in the case of W-state self-test applies:

$$\begin{aligned}
\Phi(Z_i |\psi'\rangle |0\rangle^{\otimes N}) &= |\text{junk}\rangle \otimes \sigma_{\mathrm{Z}}^{(i)} |xD_N^m\rangle \qquad (i = 1, \ldots, N-1), \\
\Phi(X_i |\psi'\rangle |0\rangle^{\otimes N}) &= |\text{junk}\rangle \otimes \sigma_{\mathrm{X}}^{(i)} |xD_N^m\rangle \qquad (i = 1, \ldots, N-1), \\
\Phi(Z_N |\psi'\rangle |0\rangle^{\otimes N}) &= |\text{junk}\rangle \otimes \left(\frac{\sigma_{\mathrm{Z}}^{(N)} + \sigma_{\mathrm{X}}^{(N)}}{\sqrt{2}} \right) |xD_N^m\rangle, \\
\Phi(X_N |\psi'\rangle |0\rangle^{\otimes N}) &= |\text{junk}\rangle \otimes \left(\frac{\sigma_{\mathrm{Z}}^{(N)} - \sigma_{\mathrm{X}}^{(N)}}{\sqrt{2}} \right) |xD_N^m\rangle.
\end{aligned}$$

Notice that our self-test exploits two observables per site and the total number of correlators one has to determine for every Dicke state in this procedure again scales linearly with N, in contrast with the exponential scaling of quantum state tomography.

4.5 Graph states

We finally demonstrate that our method applies also to the graph states. These are N-qubit quantum states that have been widely exploited in quantum information processing, in particular in quantum computing, error correction, and secret sharing (see, e.g., Ref. [Hei+06]). It is thus an interesting question to design efficient methods of their certification, in particular self-testing. Such a method was proposed in Ref. [McK14] however, in general it needs three measurements for at least one party. Below we show that the approach based on violation of the CHSH Bell inequality provides a small improvement, as it requires only two measurements at each site.

Let $|\psi_G\rangle$ be an N-qubit graph state that corresponds to a graph $G = \{V, E\}$, where $V = \{1, \ldots, N\}$ and E stand for the sets of vertices and edges, respectively. Recall that any graph state can be written in the following form

$$|\psi_G\rangle = \frac{1}{\sqrt{2^N}} \sum_{i \in \{0,1\}^N} (-1)^{\mu(i)} |i\rangle, \tag{4.71}$$

where the summation is over all sequences $i = (i_1, \ldots, i_N)$ with $i_j = 0, 1$, and $\mu(i)$ is the number of edges connecting qubits being in the state $|1\rangle$ in ket $|i\rangle$ (without counting the same edge twice).

Let then ν_i be the set of neighbours of the ith qubit, that is, all those qubits that are connected with i by an edge, while by $|\nu_i|$ we denote the number of elements in ν_i. Likewise, we denote by $\nu_{i,j}$ the set of neighbours of a pair of qubits i and j, i.e., all those qubits that are connected to either i or j (notice that $\nu_{i,j} = \nu_{j,i}$), and $|\nu_{i,j}|$ the number of elements of $\nu_{i,j}$. We also assume that the parties are labelled in such a way that qubits $N-1$ and N are connected and the party N has the smallest number of neighbours, i.e., $|\nu_N| \leq |\nu_i|$ for all i.

The main property of the graph states underlying our simple self-test is that by measuring all the neighbours of a pair of connected qubits i, j in the σ_{Z} basis, the two qubits i and j are left in one of the Bell states [cf. Prop. 1 in Ref. [HEB04]]:

$$\frac{1}{\sqrt{2}}(\sigma_{\mathrm{Z}}^{m_i} \otimes \sigma_{\mathrm{Z}}^{m_j})(|0+\rangle + |1-\rangle) \tag{4.72}$$

where m_i (m_j) is the number of parties from set $\nu_{i,j} \setminus j$ ($\nu_{i,j} \setminus i$) whose result of a measurement in σ_{Z} basis was -1, and where we have neglected an unimportant -1 factor that might appear.

Let us denote $Z^{(\tau)}_{\nu_{i,j}} = \otimes_{l \in \nu_{i,j}} Z^{(\tau_l)}_l$, where τ is an $|\nu_{i,j}|$-element sequence with each $\tau_l \in \{+,-\}$ (the operator $Z^{(\tau)}_{\nu_{i,j}}$ acts only on the parties belonging to $\nu_{i,j}$).

Theorem 8. *Let $|\psi'\rangle$ and measurements Z_i, X_i with $i = 1, \ldots, N-1$ and $D_N, E_N, Z_N \equiv \frac{D_N - E_N}{\sqrt{2}}, X_N \equiv \frac{D_N + E_N}{\sqrt{2}}$ satisfy the following conditions*

$$\left\langle Z^{(\tau)}_{\nu_{N-1,N}} \right\rangle = \frac{1}{2^{|\nu_{N-1,N}|}}, \qquad \left\langle Z^{(\tau)}_{\nu_{N-1,N}} \otimes \mathscr{B}^{(m_{N-1},m_N)}_{N-1,N} \right\rangle = \frac{2\sqrt{2}}{2^{|\nu_{N-1,N}|}} \tag{4.73}$$

for every choice of the $|\nu_{i,j}|$-element sequence τ. The Bell operators $\mathscr{B}^{(m_{N-1},m_N)}_{N-1,N}$ are defined as

$$\mathscr{B}^{(m_{N-1},m_N)}_{N-1,N} = (-1)^{m_N} X_{N-1} \otimes (D_N + E_N) + (-1)^{m_{N-1}} Z_{N-1} \otimes (D_N - E_N), \tag{4.74}$$

where m_{N-1} and m_N are the numbers of neighbours of the qubits, respectively, $N-1$ and N (excluding the Nth qubit and $N-1$th qubit, respectively) which are projected onto the eigenvector of Z_i^-.

We then assume that

$$\left\langle Z^{(\tau)}_{\nu_{i,j}} \right\rangle = \frac{1}{2^{|\nu_{i,j}|}}, \qquad \left\langle Z^{(\tau)}_{\nu_{i,j}} \otimes Z_i \otimes X_j \right\rangle = \frac{(-1)^{m_j}}{2^{|\nu_{i,j}|}} \tag{4.75}$$

for all connected pairs of indices $i \neq j$ except for $\neq (N, N-1)$. As before, $Z^{(\tau)}_{\nu_{i,j}} = \otimes_{l \in \nu_{i,j}} Z^{(\tau_l)}_l$. Then, for the isometry Φ_N one has

$$\Phi_N \left(|\psi'\rangle \, |0\rangle^{\otimes N} \right) = |\mathrm{junk}\rangle \, |\psi_G\rangle \, . \tag{4.76}$$

Proof. The conditions in Eq. (4.73) imply that the normalized state

$$|\widetilde{\psi}^{(\tau)}_{N-1,N}\rangle = \sqrt{2^{|\nu_{N-1,N}|}}\,Z^{(\tau)}_{\nu_{N-1,N}}\,|\psi'\rangle \tag{4.77}$$

violates maximally the CHSH Bell inequality, which in turn implies that

$$\{X_{N-1},Z_{N-1}\}\,|\widetilde{\psi}^{(\tau)}_{N-1,N}\rangle = 0 \quad \text{and} \quad \{X_N,Z_N\}\,|\widetilde{\psi}^{(\tau)}_{N-1,N}\rangle = 0, \tag{4.78}$$

where $X_N = (D_N + E_N)/\sqrt{2}$ and $Z_N = (D_N - E_N)/\sqrt{2}$. These identities hold true for any of $2^{|\nu_{i,j}|}$ projected states $|\widetilde{\psi}^{(\tau)}_{N-1,N}\rangle$, and therefore it must also hold for the initial state $|\psi\rangle$, i.e.,

$$\{X_{N-1},Z_{N-1}\}\,|\psi'\rangle = 0 \quad \text{and} \quad \{X_N,Z_N\}\,|\psi'\rangle = 0. \tag{4.79}$$

This is because one can always decompose $|\psi'\rangle$ in the eigenbasis of the operator $Z_{\nu_{N-1,N}}$ which is a tensor product of Z operators acting on the neighbours of i,j.

Then, let us focus on the second bunch of conditions (4.75). They imply that the length of the projected vectors $|\psi^{(\tau)}_{i,j}\rangle = Z^{(\tau)}_{\nu_{i,j}}|\psi'\rangle$ is $1/\sqrt{2^{|\nu_{i,j}|}}$, so is the norm of $Z_i\,|\psi^{(\tau)}_{i,j}\rangle$ and $X_j\,|\psi^{(\tau)}_{i,j}\rangle$ for any connected pair $i \neq j$. This together with (4.75) mean that the vectors $Z_i\,|\psi^{(\tau)}_{i,j}\rangle$ and $X_j\,|\psi^{(\tau)}_{i,j}\rangle$ are parallel or antiparallel, or, more precisely, that

$$(-1)^{m_j} Z_i\,|\psi^{(\tau)}_{i,j}\rangle = X_j\,|\psi^{(\tau)}_{i,j}\rangle \tag{4.80}$$

for any connected pair of parties $i \neq j$.

Let us now consider one of the parties connected to the party $N-1$ (there must be at least one such party as otherwise the Nth one would not be the one with the smallest number of neighbours or the graph would be bipartite). We label this vertex by $N-2$. It then follows from conditions (4.80) that for the particular pair of vertices $N-2, N-1$, one has the following identities

$$X_{N-2}\,|\psi^{(\tau)}_{N-2,N-1}\rangle = (-1)^{m_{N-2}} Z_{N-1}\,|\psi^{(\tau)}_{N-2,N-1}\rangle \tag{4.81}$$

and

$$Z_{N-2}\,|\psi^{(\tau)}_{N-2,N-1}\rangle = (-1)^{m_{N-1}} X_{N-1}\,|\psi^{(\tau)}_{N-2,N-1}\rangle \tag{4.82}$$

hold true for all configurations of τ. With their aid the following sequence of equalities

$$\begin{aligned}
X_{N-2}Z_{N-2}\,|\psi^{(\tau)}_{N-2,N-1}\rangle &= (-1)^{m_{N-1}} X_{N-2}X_{N-1}\,|\psi^{(\tau)}_{N-2,N-1}\rangle \\
&= (-1)^{m_{N-1}+m_{N-2}} X_{N-1}Z_{N-1}\,|\psi^{(\tau)}_{N-2,N-1}\rangle \\
&= -(-1)^{m_{N-1}+m_{N-2}} Z_{N-1}X_{N-1}\,|\psi^{(\tau)}_{N-2,N-1}\rangle \\
&= -(-1)^{m_{N-2}} Z_{N-1}Z_{N-2}\,|\psi^{(\tau)}_{N-2,N-1}\rangle \\
&= -Z_{N-2}X_{N-2}\,|\psi^{(\tau)}_{N-2,N-1}\rangle
\end{aligned} \tag{4.83}$$

holds true for any choice of τ, where first and the second equality stems from Eqs. (4.82) and (4.81), respectively, the third one is a consequence of the anticommutativity of X_{N-1} and Z_{N-1}. Finally, the fourth and the fifth equality follows again from Eqs. (4.82) and (4.81), respectively.

Since the identity (4.83) is obeyed for any configuration of τ, it must also hold for the state $|\psi'\rangle$, that is, $\{X_{N-2}, Z_{N-2}\}|\psi'\rangle = 0$. Taking into account the conditions (4.73), this procedure can be recursively applied to any pair of connected particles, yielding (together with (4.79))

$$\{X_i, Z_i\}|\psi'\rangle = 0 \tag{4.84}$$

for any $i = 1, \dots, N$.

The action of the isometry is given by

$$\Phi_N(|\psi'\rangle|0\rangle^{\otimes N}) = \sum_{i_1,\dots,i_N=0}^{1} X_1^{i_1} \dots X_N^{i_N} Z_1^{(i_1)} \dots Z_N^{(i_N)} |\psi'\rangle |i_1 \dots i_N\rangle \tag{4.85}$$

Let us now consider a particular term in the above decomposition in which the sequence $i_1, \dots, i_N$ has $k > 0$ ones at positions $j_1, \dots, j_k$, i.e.,

$$X_{j_1}^{i_{j_1}} \dots X_{j_k}^{i_{j_k}} \bigotimes_{l \notin I} Z_l^{(+)} \bigotimes_{l \in I} Z_l^{(-)} |\psi'\rangle, \tag{4.86}$$

where $I = \{j_1, \dots, j_k\}$. By using the previously derived relations, we want to turn this expression into one that is proportional to the junk state $Z_1^{(+)} \otimes \dots \otimes Z_N^{(+)} |\psi'\rangle$. To this end, let us first focus on the party j_k and consider one of its neighbours which we denote by l. For this pair of parties, the conditions (4.80) imply that

$$X_{j_k} |\psi_{j_k,l}\rangle = (-1)^{m_{j_k}} Z_l |\psi_{j_k,l}\rangle, \tag{4.87}$$

where, to recall, m_{j_k} is the number of neighbours of j_k being in the state $|1\rangle$ except for l. The above identity together with the anticommutativity relation $\{X_{j_k}, Z_{j_k}\}|\psi'\rangle = 0$ allow us to replace in Eq. (4.86) the operator $X_{j_k}^{i_k} Z_{j_k}^{(-)}$ by $(-1)^{m_{j_k}} Z_{j_k}^{(+)} Z_l$. Now, if the value of i_l in the corresponding ket $|i_1, \dots, i_N\rangle$ is zero, the last operator Z_l can be simply absorbed by $Z_l^{(+)}$, while if $i_l = 1$, one uses that fact that $Z_l^{(-)} Z_l = -Z_l^{(-)}$, meaning that one has an additional minus sign. Altogether this turns the operator $X_{j_k}^{i_k} Z_{j_k}^{(-)}$ into $(-1)^{m'_{j_k}} Z_{j_k}^{(+)}$, where m'_{j_k} is the number of neighbours of j_k (including i_l) which are in the state $|1\rangle$. Plugging this into Eq. (4.86) we can rewrite the latter as

$$(-1)^{m'_{j_k}} X_{j_1}^{i_{j_1}} \dots X_{j_{k-1}}^{i_{j_{k-1}}} \bigotimes_{l \notin I'} Z_l^{(+)} \bigotimes_{l \in I'} Z_l^{(-)} |\psi'\rangle, \tag{4.88}$$

where now $I' = I \setminus \{i_l\}$, and so we have lowered the number of elements of I by one. It should be stressed that this affects the numbers of neighbours of those parties that are still in I', which will be of importance for what follows.

Now, we can apply recursively the same reasoning to the remaining elements of I', keeping in mind that at each step one element is removed from I'. We thus arrive at

$$(-1)^{\mu'(i)} Z_1^{(+)} \otimes \ldots \otimes Z_N^{(+)} |\psi'\rangle, \tag{4.89}$$

with μ' defined as

$$\mu'(i) = \sum_{l=1}^{k} m_{j_l}^{>}, \tag{4.90}$$

where $m_{j_l}^{>}$ is the number of neighbours of i_{j_l} being in the state $|1\rangle$ and having smaller indices than j_l, or, in other words, those elements of $I = \{j_1, \ldots, j_k\}$ smaller than j_l that are neighbours of i_{j_l}. One immediately notices that $\mu'(i)$ equals $\mu(i)$ for a given i, and therefore by applying the above reasoning to every term in Eq. (4.85), one arrives at

$$\Phi_N(|\psi'\rangle |0\rangle^{\otimes N}) = \left(Z_1^{(+)} \otimes \ldots \otimes Z_N^{(+)} |\psi'\rangle\right) \otimes \sum_i (-1)^{\mu(i)} |i\rangle, \tag{4.91}$$

which after normalizing both terms can be written as

$$\Phi_N(|\psi'\rangle |0\rangle^{\otimes N}) = |\text{junk}\rangle |\psi_G\rangle \tag{4.92}$$

with $|\text{junk}\rangle = (1/\sqrt{2^N})(Z_1^{(+)} \otimes \ldots \otimes Z_N^{(+)} |\psi'\rangle)$.

Once relation (4.84) is satisfied for all is the proof for measurement self-testing goes along the same lines as the proof for the self-testing of the state. Let us check how isometry Φ_n acts on the state $X_{\tilde{i}}|\psi'\rangle$. Eq. (4.88) takes the form:

$$\begin{aligned}
\Phi_N(X_{\tilde{i}}|\psi'\rangle |0\rangle^{\otimes N}) &= \sum_{I,l} (-1)^{m'_{j_k}} X_{j_1}^{i_{j_1}} \ldots X_{j_{k-1}}^{i_{j_{k-1}}} \bigotimes_{l \notin I'} Z_l^{(+)} \bigotimes_{l \in I'} Z_l^{(-)} X_{\tilde{i}} |\psi'\rangle \\
&= \sum_{I \oplus \tilde{i}, l} (-1)^{m'_{j_k}+1} X_{j_1}^{i_{j_1}} \ldots X_{j_{k-1}}^{i_{j_{k-1}}} \bigotimes_{l \notin I'} Z_l^{(+)} \bigotimes_{l \in I'} Z_l^{(-)} |\psi'\rangle \\
&= \left(Z_1^{(+)} \otimes \ldots \otimes Z_N^{(+)} |\psi'\rangle\right) \otimes \sum_i (-1)^{\mu(i \oplus \tilde{i})} |i\rangle \\
&= |\text{junk}\rangle \otimes \sigma_{\text{X}}{}^{(\tilde{i})} |\psi_G\rangle, \quad \forall \tilde{i} \in \{1, 2, \ldots, N-1\}
\end{aligned}$$

where $I \oplus \tilde{i}$ is equal to $I/\tilde{i}$ if $\tilde{i} \in I$ and to $I \cup \tilde{i}$ otherwise, and $\mu(i \oplus \tilde{i})$ is the number of edges connecting qubits being in the state $|1\rangle$ in ket $|i \oplus (0 \ldots 0\tilde{i}0 \ldots 0)\rangle$ (without counting the same edge twice). Similarly it can be shown that

$$\begin{aligned}
\Phi_N(Z_{\tilde{i}}|\psi'\rangle |0\rangle^{\otimes N}) &= |\text{junk}\rangle \otimes \sigma_{\text{Z}}{}^{(\tilde{i})} |\psi_G\rangle, \quad \forall \tilde{i} \in \{1, 2, \ldots, N\}, \\
\Phi_N(D_N |\psi'\rangle |0\rangle^{\otimes N}) &= |\text{junk}\rangle \otimes \left(\frac{\sigma_{\text{X}}^{(N)} + \sigma_{\text{Z}}^{(N)}}{\sqrt{2}}\right) |\psi_G\rangle, \\
\Phi_N(E_N |\psi'\rangle |0\rangle^{\otimes N}) &= |\text{junk}\rangle \otimes \left(\frac{-\sigma_{\text{X}}^{(N)} + \sigma_{\text{Z}}^{(N)}}{\sqrt{2}}\right) |\psi_G\rangle.
\end{aligned}$$

□

Finally, note that for self-testing graph-states one has to measure $3+|E|$ correlators, where $|E|$ is the total number of edges, which even for the fully connected graph is strictly better scaling than the complexity of quantum state tomography.

4.6 Discussion

We investigated a simple, but potentially general, approach to self-testing multipartite states, inspired by [Wu+14], which relies on the well understood method of self-testing bipartite qubit states based on the maximal violation of the tilted CHSH Bell inequality. This approach allows one to self-test, with few measurements, all permutationally-invariant Dicke states, all partially entangled GHZ qubit states, and to recover self-testing of graph states (which was previously known through stabilizer-state methods). In our work, we also generalize self-testing of partially entangled GHZ qubit states to the qudit case, using techniques from [CGS17]. We obtain the first self-testing result for a class of multipartite qudit states, by showing that all multipartite qudit states that admit a Schmidt decomposition can be self-tested. Importantly, our self-tests have a low complexity in terms of resources as they require up to four measurement choices per party, and the total number of correlators that one needs to determine scales linearly with the number of parties.

As a direction for future work, we are particularly interested in extending this approach to self-test any generic multipartite entangled state of qubits (which is local-unitary equivalent to its complex conjugate in any basis). The main challenge here is to provide a general recipe to construct a single isometry that self-tests the global state from the different ones derived from various subtests (i.e. from projecting various subsets of parties and looking at the correlations of the remaining ones). This appears to be challenging for states that do not have any particular symmetry.

Finally, notice that all presented self-tests which rely on the maximal violation of the CHSH Bell inequality can be restated and proved in terms of the other available self-tests. In particular, any self-test discussed in [WWS16] would work in case of two measurements per site, and self-tests in [ŠASA16] would work for higher number of inputs.

Chapter 5

Self-testing through EPR-steering

In Chapter 2 we learned that a nonlocal probability distribution witnesses in a device-independent manner the presence of entanglement in the system. The protocol of entanglement detection can be lifted to the self-testing - certifying the presence of a specific entangled state. Both, entanglement detection and self-testing, draw its conclusions from a violation of an adequate Bell inequality; any violation suffices for the former, while the maximal is necessary for the latter. In the two previous chapters we saw how different quantum states can be self-tested with the aid of different Bell inequalities or in some cases specific nonlocal behaviours. All the self-testing protocols we encountered are by construction device-independent. On the middle ground, we saw that entanglement can also be witnessed through EPR-steering. A natural question is whether one can perform robust self-testing in such a scenario? This is obviously true since we can check the violation of the adequate Bell inequality when the trusted party performs exactly the measurements leading to the maximal violation. A better question is whether it is vastly more advantageous to consider self-testing in this scenario? In this chapter we address this question.

5.1 Motivation and technical preliminaries

Before moving to the main contributions, let us motivate this self-testing scenario from the standpoint of quantum information. One of the tasks which can make use of EPR-steering scenarios is blind quantum computing (BQC). This task is relevant when a client having access to a limited quantum operations wants to securely delegate a computation to a ”server” who has a full-power quantum computer [BFK09, RUV13]. Security consists in inability of the server to learn, nor the input to the computation, neither the particular computation itself. Another task, utilising EPR-steering is one-sided device-independent quantum key distribution, differing from the standard DIQKD in the fact that one party can trust its devices [Bra+12, Wal+16]. Finally let us mention randomness certification in quantum networks which can be more easily performed if some parties trust their devices [Mat+17].

Motivated by terminology from BQC, instead of Alice and Bob, we will name two involved parties, a client and a user. Since the client now has characterized and trusted devices in their laboratory, they can perform quantum state tomography. As we saw in Section 2.4, in EPR-steering the object of study becomes an assemblage: the set of client's reduced states conditioned on a measurement made on the provider's side. Self-testing inferred from an assemblage will be denoted as *robust assemblage-based one-sided self-testing* (AST), where "one sided" indicates that the operating scenario is one-sided device-independent. In the following sections we will show that AST can be achieved with the physical state being at least $O(\sqrt{\varepsilon})$-close to the reference state if the observed elements of an assemblage are ε-close to the ideal elements (where distance in both cases is the trace distance). Additionally, the client can perform some measurements on the elements of an assemblage, obtaining in this way correlations between the client and the provider. Self-testing obtained from these correlations will be called *robust correlation-based one-sided self-testing* (CST).

Standard self-testing implies CST so the latter scenario will never perform any worse than the former. Additionally, CST implies AST so the latter truly captures the novel capabilities in the formalism. In this chapter, when it comes to self-testing we show both analytically and numerically that one can do better in the framework of CST and AST as compared to current methods in conventional self-testing. This is not surprising since by trusting one side, we should have access to more information about the physical state. On the other hand, we show that improvement is not as big as we would like. To put it more precisely, if the assemblage is, in some sense, ε-close to the ideal assemblage, we can only establish $O(\sqrt{\varepsilon})$-closeness of the physical experiment to the reference one. This quadratic difference is also shown to be a general limitation and not just a limitation of our specific methods. In this way, from the point-of-view of self-testing, EPR-steering behaves asymptotically in the same way as Bell nonlocality.

We indicate where AST and CST could also prove advantageous over standard self-testing and this is in the case of establishing the structure of sub-systems within multipartite quantum states. That is, in certain self-testing proofs a lot of work and resources goes into establishing that untrusted devices have quantum systems that are essentially independent from one another. In addition to considering the self-testing of a bipartite quantum state, we show that one can get further improvements by establishing a tensor product structure between sub-systems. This could be where the essential novelties of AST and CST lie.

Aside from work in the remit of self-testing there is other work in the direction of entanglement verification between many parties. For example, Pappa *et al* show how to verify GHZ states among n parties if some of them can be trusted while others not [PCWDK12]. Their verification proofs boil down to establishing the probability with which the quantum state passes a particular test given the state's distance from the ideal case. This can be seen as going in the other direction compared to CST, where we ask how close a state is to ideal if we pass a test (demonstrating some ideal correlations) with a particular probability. Our work thus nicely complements some of the existing methods in this direction.

Another line of research that is related to our own is to characterize (non-local) quantum correlations given assumptions made about the dimension of the Hilbert space for one of the parties [NDV14]. This assumption of limiting the dimension is a relaxation of the assumption that devices in one of the parties' laboratories are trusted. These works are relevant for semi-device-independent quantum cryptography and device-independent dimension witnesses [PB11, GBHA10].

5.1.1 General set-up

For simplicity and relevance we restrict ourselves to the bipartite scenarios. In Sec. 5.6 we will extend the framework to multipartite systems. In our setting (see Fig. 5.1), the client and the provider share both quantum and classical communication channels and all devices are assumed to satisfy the laws of quantum theory. Henceforth, the shared state lives in the tensor product of the finite-dimensional Hilbert spaces $\mathscr{H}^{\mathrm{C}}$ (client's share) and $\mathscr{H}^{\mathrm{P}}$ (provider's share). The provider uses the quantum communication channel to send a quantum system to the client, so they share a quantum state $\rho^{\mathrm{CP}} \in \mathbb{B}(\mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{P}})$. Crucially, in our scenario, the dimension of the Hilbert space $\mathscr{H}^{\mathrm{C}}$ is known but the space $\mathscr{H}^{\mathrm{P}}$ can have an unrestricted dimension since we do not, in general, trust the provider. Therefore, without loss of generality we can work with the pure states $\rho^{\mathrm{CP}} = |\psi'\rangle\langle\psi'|$, since we can always dilate the space $\mathscr{H}^{\mathrm{P}}$ to find an appropriate purification. The client uses the classical communication channel to ask the provider to perform a measurement labelled by $x \in \{1, \cdots, d\}$. For each measurement, there are $k \in \mathbb{N}$ possible outcomes labelled by the symbol $a \in \{0, 1, 2, ..., (k-1)\}$, and the provider sends back to the client the measurement outcome they obtained. Again, since the dimension of $\mathscr{H}^{\mathrm{P}}$ is unrestricted, we assume that measurement operators $\{M'_{a|x}\}$ are projective.

Conditioned on each measurement outcome a given the choice x, the client performs state tomography on their part of the state $|\psi'\rangle$ and obtains the assemblage elements $\sigma'_{a|x} = \mathrm{tr}_{\mathrm{P}}\left(\mathbb{1}^{\mathrm{C}} \otimes M'_{a|x} |\psi'\rangle\langle\psi'|\right)$. Recall that the elements of assemblage satisfy no-signalling relation $\sum_a \sigma'_{a|x} = \mathrm{tr}_{\mathrm{P}}(|\psi'\rangle\langle\psi'|) = \rho'^{\mathrm{C}}$, where ρ'^{C} is the reduced state of the client's system. One can extract the probability $p(a|x)$ of the provider's measurement

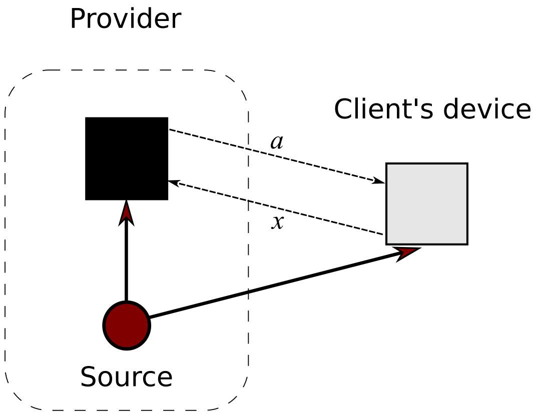

Figure 5.1: In our framework we have a client who has direct access to his part of the quantum system generated by the source in the provider's laboratory. We can also ask the provider to perform a measurement labelled by x and generate an outcome labelled by a all the while treating the provider's measurement device and the source as a black box. The dotted lines denote classical channels, while full lines represents a quantum channel

outcome a for the choice x by taking $\mathrm{tr}(\sigma'_{a|x}) = p(a|x)$.

The experiment can be equivalently characterized by the correlations between the client and provider where both parties make measurements and look at the conditional probabilities $p(a,b|x,y)$ where $y \in \{0,1,...,(d-1)\}$ is the client's choice of measurement and $b \in \{0,1,2,...,(k-1)\}$ the outcome for that choice. If the client performs POVMs $\{N_{b|y}\}$, then these correlations can be readily obtained from elements of the assemblage as $p(a,b|x,y) = \mathrm{tr}\left(N_{b|y}\sigma'_{a|x}\right)$.

As in the previous chapters, the reference experiment is denoted with un-primed letters $\{M_{a|x}, N_{b|y}, |\psi\rangle\}$, as opposed to the above defined physical experiment $\{M'_{a|x}, N'_{b|y}, |\psi'\rangle\}$. The aim is to show the equivalence (2.24) between the reference and the physical experiment.

5.2 Reduced states and the purification principle

It may seem that self-testing in the scenario defined here is a trivial task due to the Schrödinger-HJW thorem [Sch36, HJW93], which says that every density matrix ρ^{A} can result as the reduced state of some bipartite pure state $|\psi\rangle^{\mathrm{AB}}$ on a joint system, according to $\rho^{\mathrm{A}} = \mathrm{tr}_{\mathrm{B}}(|\psi\rangle\langle\psi|^{\mathrm{AB}})$, and this pure state is uniquely defined up to a unitary transformation on system B. Analogously, in our formalism, the reduced state $\rho'^{\mathrm{C}} = \mathrm{tr}_{\mathrm{P}}(|\psi'\rangle\langle\psi'|)$ can be described by the state $|\psi'\rangle$ up to a unitary on the provider's system. More precisely, from the density matrix $\rho'^{\mathrm{C}} = \sum_i \lambda_i \left|\mu_i\right\rangle \left\langle\mu_i\right|$ (such that $\sum_i \lambda_i = 1$ and $\lambda_i \geq 0$ for all i) we can easily get the Schmidt decomposition of the purification:

$$\left|\psi'\right\rangle = \sum_i \sqrt{\lambda_i} \left|\mu_i\right\rangle \left|\nu_i\right\rangle$$

where $\{\left|\mu_i\right\rangle\}_i$ ($\{\left|\nu_i\right\rangle\}_i$) is some set of orthogonal states in $\mathscr{H}^{\mathrm{C}}$ ($\mathscr{H}^{\mathrm{P}}$).

Consequently, we can ensure equivalence between $\left|\psi\right\rangle$ and $\left|\psi'\right\rangle$ solely by checking if the reduced state $\rho_{\mathrm{C}} = \mathrm{tr}_{\mathrm{P}}(\left|\psi\right\rangle\left\langle\psi\right|)$ is the same as the reduced state $\rho'_{\mathrm{C}} = \mathrm{tr}_{\mathrm{P}}(\left|\psi'\right\rangle\left\langle\psi'\right|)$. Note that just from the fact that ρ'^{C} is mixed the client may be sure that they share some entanglement with the provider. This is purely a consequence of the assumption that they share a pure state. Indeed, in cryptographic scenario it is well-motivated to assume that the provider produces a pure state since this gives them *maximal information* about the devices that are used in a protocol.

Even though self-testing of states is rendered easy by our assumptions, the self-testing of measurements does not follow from only looking at the reduced state ρ'^{C}. In other words, knowing the global pure $\left|\psi'\right\rangle$ from the reduced state ρ'^{C}, does not immediately imply that the provider is making the required measurements on a useful part of that pure state. It should be emphasized that in any one-sided device-independent quantum information protocol, measurements will be made on a state in any task to extract classical information from the systems, both trusted and untrusted. The self-testing of measurements made by an untrusted agent is, as explicitly stated in Eq. (2.24), crucial. We give a simple example to illustrate this point. This is an example of a physical system that a provider can prepare and a measurement they can perform.

Example 8.1. *Establishing that the client and the provider share a state that is equivalent to a reference state is not immediately useful. Consider the situation where the provider prepares the state* $\left|\psi'\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0^{\mathrm{C}}\right\rangle\left|0^{\mathrm{P}_1}\right\rangle\left|0^{\mathrm{P}_2}\right\rangle + \left|1^{\mathrm{C}}\right\rangle\left|1^{\mathrm{P}_1}\right\rangle\left|0^{\mathrm{P}_2}\right\rangle\right)$ *where the subscripts* P_1 *and* P_2 *label two qubits that the provider retains and sends the qubit with the subscript* Cc *to the client. The two qubits labelled by* P_1 *and* P_2 *can be jointly measured or individually measured. In this example the provider's measurement solely consists of measuring qubit* P_2 *and ignoring qubit* P_1 *such that measurement projectors are of the form* $\mathbb{1}_{\mathrm{P}_1} \otimes (M'_{a|x})^{\mathrm{P}_2}$. *Therefore, the reduced state of the client is* $\rho^{\mathrm{C}} = \frac{\mathbb{1}}{2}$ *which indicates that the client and provider share a maximally entangled state. However, every element of the assemblage* $\{\sigma'_{a|x}\}_{a,x}$ *is* $\sigma_{a|x} = \frac{\mathbb{1}}{2}$, *and thus unaffected by any measurement performed by the provider. Therefore we cannot say anything about the provider's measurements and, furthermore, the entanglement is not being utilized by the provider and will thus not be useful for any quantum information task.*

This example just highlights that in our scenario it only makes sense to establish equivalence between a physical experiment and reference experiment taking into account *both* *the state and measurements*. The example motivates the need to study the assemblage generated in our scenario and not just the reduced state. Also, as will be shown later, this allows us to construct explicit isometries demonstrating equivalence between a physical and reference experiment instead of just knowing that such an isometry exists. In colloquial terms, being able to explicitly construct an isometry allows one to be able to "locate" their desired state within the physical state.

So far we have assumed perfect equivalence between the reference and physical experiment as described by Eqs. (2.24). In Sec. 5.3 we extend our discussion to the case where equivalence can be established approximately which is known as robust self-testing. Instead of using the reduced state of the client and assemblage, we may wish to study self-testing given the correlations resulting from measurements on the assemblage and we discuss this in Sec. 5.4.

5.3 Robust assemblage-based one-sided self-testing

In this section we formally introduce *robust assemblage-based one-sided self-testing* (AST) and discuss its advantages and limitations. For discussing robustness we first need to decide about the appropriate distance measure when it comes to assemblages. Since elements of an assemblage are operators on a Hilbert space, we will use the Schatten 1-norm $\|A\|_1$ for $A \in L(\mathscr{H})$ being a linear operator acting on $\mathscr{H}$. This norm is directly related to $D(\rho,\sigma)$, the trace distance between quantum states since

$$D(\rho,\sigma) = \frac{1}{2}\|\rho - \sigma\|_1$$

for density matrices ρ and σ. Equivalently,

$$D(\rho,\sigma) = \frac{1}{2}\sum_i |\lambda_i|$$

where λ_i is the i-th eigenvalue of the operator $(\rho - \sigma)$. The trace distance has even simpler form when $\rho = |a\rangle\langle a|$ and $\sigma = |b\rangle\langle b|$ are pure [NC00]:

$$D(|a\rangle\langle a|, |b\rangle\langle b|) = \sqrt{1 - |\langle a|b\rangle|^2}.$$

A distance measure is introduced for consideration of imperfect experiments. The task is to infer closeness of our physical and reference experiments if their predictions differ by a small amount. In this formalism we will use the trace distance to estimate closeness between the physical state $|\psi'\rangle$ and reference state $|\psi\rangle$. Thus, if $D(\rho'^{\mathrm{C}}, \rho^{\mathrm{C}}) = \varepsilon > 0$ where $\rho^{\mathrm{C}} = \mathrm{tr}_{\mathrm{P}}(|\psi\rangle\langle\psi|)$, then the minimal distance between physical and reference states, allowing for isometries Φ on the provider's side, will be the minimal value of

$$D\left(|\Phi\rangle\langle\Phi|, |\mathrm{junk}\rangle\langle\mathrm{junk}| \otimes |\psi\rangle\langle\psi|\right) = \sqrt{1 - |\langle\mathrm{junk}| \otimes \langle\psi|\Phi\rangle|^2} \tag{5.1}$$

for $|\Phi\rangle = \Phi(|\psi'\rangle)$. Clearly,

$$D(|\Phi\rangle\langle\Phi|, |\text{junk}\rangle\langle\text{junk}| \otimes |\psi\rangle\langle\psi|) \geq D(\rho^{\text{C}}, \rho'^{\text{C}}) = \varepsilon \tag{5.2}$$

since the trace distance does not increase when tracing out the provider's sub-system.

The lower bound given in Eq. (5.2) does not tell us if an isometry achieving it exists at all. Our aim is to be able to prove that there is an isometry for which the distance from Eq. (5.1) is small. Moreover, it would be good if we can construct such an isometry. We now formalize this intuition in the following definition:

Definition 8.1. *Given a reference experiment consisting of the state $|\psi\rangle \in \mathscr{H}^{\text{C}} \otimes \mathscr{H}'^{\text{P}}$ with reduced state ρ^{C} and measurements $\{M_{a|x}\}_{a,x}$ such that the assemblage $\{\sigma_{a|x}\}_{a,x}$ has elements $\sigma_{a|x} = \text{tr}_{\text{P}}\left[(\mathbb{1}^{\text{C}} \otimes M_{a|x})|\psi\rangle\langle\psi|\right]$, $\forall$ a, x. Also given a physical experiment with the state $|\psi'\rangle \in \mathscr{H}^{\text{C}} \otimes \mathscr{H}^{\text{P}}$, reduced state ρ'^{C} and measurements $\{M'_{a|x}\}_{a,x}$ such that the assemblage $\{\sigma'_{a|x}\}_{a,x}$ has elements $\sigma'_{a|x} = \text{tr}_{\text{P}}\left[(\mathbb{1}^{\text{C}} \otimes M'_{a|x})|\psi'\rangle\langle\psi'|\right]$, $\forall$ a, x. Let there is a real, positive number ε such that $D(\rho^{\text{C}}, \rho'^{\text{C}}) \leq \varepsilon$ and $\|\sigma_{a|x} - \sigma'_{a|x}\|_1 \leq \varepsilon$, for all a, x. Then $f(\varepsilon)$**-robust assemblage-based one-sided self-testing ($f(\varepsilon)$-AST) is possible** if the assemblage $\{\sigma'_{a|x}\}_{a,x}$ implies that there exists an isometry $\Phi : \mathscr{H}^{\text{P}} \to \mathscr{H}^{\text{P}} \otimes \mathscr{H}'^{\text{P}}$ such that*

$$\begin{gathered} D\left(|\Phi\rangle\langle\Phi|, |\text{junk}\rangle\langle\text{junk}| \otimes |\psi\rangle\langle\psi|\right) \leq f(\varepsilon), \\ \| |\Phi, M'_{a|x}\rangle\langle\Phi, M'_{a|x}| - |\text{junk}\rangle\langle\text{junk}| \otimes (\mathbb{1}^{\text{C}} \otimes M_{a|x})|\psi\rangle\langle\psi|(\mathbb{1}^{\text{C}} \otimes M_{a|x})\|_1 \leq f(\varepsilon) \end{gathered} \tag{5.3}$$

for $|\Phi\rangle = \Phi(|\psi'\rangle)$, $|\Phi, M'_{a|x}\rangle = \Phi(\mathbb{1}^{\text{C}} \otimes M'_{a|x}|\psi'\rangle)$, $|\text{junk}\rangle \in \mathscr{H}^{\text{P}}$ and $f : \mathbb{R} \to \mathbb{R}$.

In this definition, for the sake of simplicity, we have introduced the same function $f(\varepsilon)$ as the bound for all the distances in the experiment. It will often be the case that the trace distance between reduced states will be smaller than the distance between the assemblage elements, but we are considering the *worst case* analysis. In further study, it could be of interest to give a finer distinction between these distance measures in the definition. Note also that, in this definition, we only claim the existence of an isometrtry, without specifying its nature. Later, in Sec. 5.5, we will deal with constructing an explicit isometry. Also, robust self-testing makes sense, and justifies its name, if the function f is not too steep, i.e. if $f(\varepsilon) \leq O(\varepsilon^{\frac{1}{p}})$ where p is upper-bounded by a small positive integer. Since $D(\rho^{\text{C}}, \rho'^{\text{C}}) = \varepsilon$ establishes a lower bound on the distance between physical and reference experiments, the ideal case would be $O(\varepsilon)$-AST. Unfortunately such bound is not possible, which we show by constructing a simple example contradicting it.

Example 8.2. *The client has a three-dimensional Hilbert space $\mathscr{H}^{\text{C}}$. The reference experiment consists of the state $|\psi\rangle^{\text{CP}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with measurements $\{M^{\text{P}}_{0|0} = |0\rangle\langle 0|, M^{\text{P}}_{1|0} = |1\rangle\langle 1|, M^{\text{P}}_{0|1} = |+\rangle\langle +|, M^{\text{P}}_{1|1} = |-\rangle\langle -|\}$ and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ where*

$\mathscr{H}'^{\mathrm{P}}$ is a two-dimensional Hilbert space. The assemblage for this reference experiment has the following elements:

$$\sigma^{\mathrm{C}}_{0|0} = \frac{1}{2}\left|0\right\rangle\left\langle 0\right|, \qquad \sigma^{\mathrm{C}}_{1|0} = \frac{1}{2}\left|1\right\rangle\left\langle 1\right|,$$
$$\sigma^{\mathrm{C}}_{0|1} = \frac{1}{2}\left|+\right\rangle\left\langle +\right|, \qquad \sigma^{\mathrm{C}}_{1|1} = \frac{1}{2}\left|-\right\rangle\left\langle -\right|.$$

The physical experiment consists of the state $\left|\psi'\right\rangle^{\mathrm{CPP}'} = \sqrt{1-\varepsilon}\left|\psi\right\rangle\left|0\right\rangle + \sqrt{\varepsilon}\left|\xi\right\rangle\left|1\right\rangle$ where $\left|\xi\right\rangle^{\mathrm{CP}} = \left|20\right\rangle$ and the subscript P' denotes a second qubit that the provider has in their possession. The measurements in the physical experiment are $M'^{\mathrm{PP}'}_{i|j} = M^{\mathrm{P}}_{i|j} \otimes \left|0\right\rangle\left\langle 0\right|^{\mathrm{P}'} + \left|i\right\rangle\left\langle i\right|^{\mathrm{P}} \otimes \left|1\right\rangle\left\langle 1\right|^{\mathrm{P}'}$ for $i \in \{0,1\}$. The state $\left|\psi'\right\rangle$ has the reduced state $\rho'^{\mathrm{C}} = \frac{(1-\varepsilon)}{2}(\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|) + \varepsilon\left|2\right\rangle\left\langle 2\right|$ thus implying that $D(\rho'^{\mathrm{C}}, \rho^{\mathrm{C}}) = \varepsilon$. The assemblage for this physical experiment then has the elements:

$$\sigma'^{\mathrm{C}}_{0|0} = \frac{(1-\varepsilon)}{2}\left|0\right\rangle\left\langle 0\right| + \varepsilon\left|2\right\rangle\left\langle 2\right|, \qquad \sigma'^{\mathrm{C}}_{1|0} = \frac{(1-\varepsilon)}{2}\left|1\right\rangle\left\langle 1\right|,$$
$$\sigma'^{\mathrm{C}}_{0|1} = \frac{(1-\varepsilon)}{2}\left|+\right\rangle\left\langle +\right| + \varepsilon\left|2\right\rangle\left\langle 2\right|, \qquad \sigma'^{\mathrm{C}}_{1|1} = \frac{(1-\varepsilon)}{2}\left|-\right\rangle\left\langle -\right|.$$

From the above assemblages we observe that $\|\sigma_{a|x} - \sigma'_{a|x}\|_1 < \frac{3}{2}\varepsilon = \varepsilon'$, for all a, x. Here we have just defined a new closeness parameter ε' for the convenience of our definitions. Given these physical and reference experiments, we now wish to calculate a lower bound on $D\left(\left|\Phi\right\rangle\left\langle\Phi\right|, \left|\mathrm{junk}\right\rangle\left\langle\mathrm{junk}\right| \otimes \left|\psi\right\rangle\left\langle\psi\right|\right)$ for all possible isometries Φ in the definition above; this will give a lower-bound on the function $f(\varepsilon')$ for $f(\varepsilon')$-AST. To do this, we introduce the notation $|\tilde{0}\rangle$ for the ancillae that the provider can introduce and U as the unitary that they can perform jointly on the ancillae and their share of the physical state $\left|\psi\right\rangle$. This then gives us:

$$D\left(U\left(\left|\psi'\right\rangle\left\langle\psi'\right| \otimes |\hat{0}\rangle\langle\hat{0}|\right)U^{\dagger}, \left|\mathrm{junk}\right\rangle\left\langle\mathrm{junk}\right| \otimes \left|\psi\right\rangle\left\langle\psi\right|\right) = \sqrt{1-F^2},$$

where

$$\begin{aligned} F &= \left|\left\langle\mathrm{junk}\right|\left\langle\psi\right|U\left|\psi'\right\rangle|\hat{0}\rangle\right| \\ &= \frac{\sqrt{1-\varepsilon}}{2}\left|\left\langle\mathrm{junk}\right|\left(\langle 0^{\mathrm{C}}0^{\mathrm{P}}|\left(\mathbb{1}^{\mathrm{C}} \otimes U\right)|0^{\mathrm{C}}0^{\mathrm{P}}\rangle + \langle 1^{\mathrm{C}}1^{\mathrm{P}}|\left(\mathbb{1}^{\mathrm{C}} \otimes U\right)|1^{\mathrm{C}}1^{\mathrm{P}}\rangle\right)|\hat{0}\rangle\right|, \end{aligned}$$

where $\mathbb{1}^{\mathrm{C}}$ is the identity on the client's system. Thus maximizing this quantity for all isometries, we obtain the maximal value $F^* = \sqrt{1-\varepsilon} = \sqrt{1-\frac{2\varepsilon'}{3}}$ and the lower bound $D\left(\left|\Phi\right\rangle\left\langle\Phi\right|, \left|\mathrm{junk}\right\rangle\left\langle\mathrm{junk}\right| \otimes \left|\psi\right\rangle\left\langle\psi\right|\right) \geq \sqrt{\frac{2\varepsilon'}{3}}$.

This example excludes the possibility of having $O(\varepsilon)$-AST given that the client's Hilbert space is three-dimensional. We will later return to this reference experiment in Sec. 5.5.1 with the modification that the client's Hilbert space is two-dimensional.

5.4 Robust correlation-based one-sided self-testing

As outlined earlier, EPR-steering can be studied from the point-of-view of the probabilities obtained from measurements performed on elements of an assemblage, i.e. known measurements made by the trusted party. This point-of-view is native to Bell non-locality and is suitable for making further parallels between non-locality and EPR-steering. In this regard one can construct EPR-steering inequalities (the EPR-steering analogues of Bell inequalities) which can be written as a linear combination of the measurement probabilities [CJWR09]. The two figures-of-merit, assemblages and measurement correlations, lead to a certain duality in the theory of EPR-steering. The approach that one will use depends on the underlying scenario. In the case when correlations are obtained by performing a tomographically complete set of measurements (on the trusted system) the two approaches become completely equivalent. However, in some cases probabilities obtained by performing a tomographically incomplete set of measurements, or even just the amount of violation of some steering inequality can provide all necessary information. Another possibility is that a trusted party can perform only two measurements and nothing more, i.e. has no resources to perform complete tomography. In this section we consider the definition and utility of defining robust self-testing with respect to these probabilities for an appropriate notion of robustness. This approach to self-testing is not immediately equivalent to the notion of AST defined previously (even if tomographically complete measurements are made) for reasons that will be become clear.

Recall the probabilities $p'(a,b|x,y) = \mathrm{tr}(N_{b|y}\sigma'_{a|x})$ for $N_{b|y}$ being elements of a general measurement associated with the outcome b for measurement choice y such that $\sum_b N_{b|y} = \mathbb{1}^{\mathrm{C}}$. Naturally, we can also obtain the probabilities $p'(b|y) = \mathrm{tr}(N_{b|y}\rho'^{\mathrm{C}})$. In addition to the "physical probabilities" $p(a,b|x,y)$, we have the "reference probabilities" $\{p(a,b|x,y)\}$ which refer to the probabilities resulting from making the same measurements $\{N_{b|y}\}_{b,y}$ on a reference assemblage $\{\sigma_{a|x}\}$ as described above. Performing robust self-testing given these probabilities will be the focus of this section.

A useful definition of the Schatten 1-norm is $\|A\|_1 = \sup_{\|B\|\leq 1}|\mathrm{tr}(BA)|$ where $\|\cdot\|$ is the operator norm. Since $F_{b|y}$ is a positive operator with operator norm upper bounded by 1 and if $D(\rho'^{\mathrm{C}}, \rho^{\mathrm{C}}) \leq \varepsilon$ and for all elements $\sigma'_{a|x}$ of an assemblage $\|\sigma_{a|x} - \sigma'_{a|x}\|_1 \leq \varepsilon$ we can conclude that

$$|p(a,b|x,y) - p'(a,b|x,y)| = |\mathrm{tr}\left[N_{b|y}\left(\sigma_{a|x} - \sigma'{}_{a|x}\right)\right]| \leq \|\sigma_{a|x} - \sigma'_{a|x}\|_1 \leq \varepsilon,$$
$$|p'(b|y) - p(b|y)| = |\mathrm{tr}\left[N_{b|y}\left(\rho'^{\mathrm{C}} - \rho^{\mathrm{C}}\right)\right]| \leq 2D(\rho'^{\mathrm{C}}\rho^{\mathrm{C}}) \leq 2\varepsilon$$

for all a, b, x, y. This then establishes that closeness of the reference and the physical assemblages implies closeness in the probabilities obtained from both experiments. Clearly, the converse is not necessarily true and closeness in probabilities does not always imply closeness of reduced states and assemblages. Assemblages can be calculated from the statistics obtained by performing tomographically complete measurements, and then the distance (in Schatten 1-norm) between this assemblage and some ideal assemblage can be calculated. However, even for tomographically complete measurements $\{N_{b|y}\}_{b,y}$, we only have that $|\mathrm{tr}\left[N_{b|y}\left(\sigma'_{a|x} - \sigma_{a|x}\right)\right]| \leq \|\sigma_{a|x} - \sigma'_{a|x}\|_1$ thus having $|\mathrm{tr}\left[N_{b|y}\left(\sigma'_{a|x} - \sigma_{a|x}\right)\right]| \leq \varepsilon$ does not imply $\|\sigma_{a|x} - \sigma'_{a|x}\|_1 \leq \varepsilon$. This goes to show that the AST approach is distinct from solely looking at the difference between probabilities.

Inspired by the literature in standard self-testing (see, e.g. Refs. [MYS14, RUV13]), it should still be possible to attain robust self-testing based on probabilities for measurements on assemblages and with this in mind, we give the following definition:

Definition 8.2. *Given a reference experiment consisting of the state $|\psi\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}'^{\mathrm{P}}$ with reduced state ρ^{C} and measurements $\{M_{a|x}\}_{a,x}$ such that the assemblage $\{\sigma_{a|x}\}_{a,x}$ has elements $\sigma_{a|x} = \mathrm{tr}_{\mathrm{P}}\left(\mathbb{1}^{\mathrm{C}} \otimes M_{a|x}|\psi\rangle\right)$, $\forall$ a, x. Also given a physical experiment with the state $|\psi'\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{P}}$, reduced state ρ'^{C} and measurements $\{M'_{a|x}\}_{a,x}$ such that the assemblage $\{\sigma'_{a|x}\}_{a,x}$ has elements $\sigma'_{a|x} = \mathrm{tr}_{\mathrm{P}}\left(\mathbb{1}^{\mathrm{C}} \otimes M'_{a|x}|\psi'\rangle\right)$, $\forall$ a, x. Additionally given a set $\{N_{b|y}\}_{b,y}$ of general measurements that act on $\mathscr{H}^{\mathrm{C}}$ such that $p'(a,b|x,y) = \mathrm{tr}\left(N_{b|y}\sigma'_{a|x}\right)$ and $p(a,b|x,y) = \mathrm{tr}\left(N_{b|y}\sigma_{a|x}\right)$ $\forall$ a, x. If, for some real $\varepsilon > 0$,*

$$\begin{aligned} |p(a,b|x,y) - p'(a,b|x,y)| &\leq \varepsilon, \\ |p(b|y) - p'(b|y)| &\leq \varepsilon, \\ |p(a|x) - p'(a|x)| &\leq \varepsilon, \end{aligned}$$

*$\forall$ a, x, b, y, then $f(\varepsilon)$**-robust correlation-based one-sided self-testing ($f(\varepsilon)$-CST)** is possible if the probabilities imply that there exists an isometry $\Phi : \mathscr{H}^{\mathrm{P}} \to \mathscr{H}^{\mathrm{P}} \otimes \mathscr{H}'^{\mathrm{P}}$ such that*

$$\begin{aligned} D\left(|\Phi\rangle\langle\Phi|, |\mathrm{junk}\rangle|\psi\rangle\langle\mathrm{junk}|\langle\psi|\right) &\leq f(\varepsilon), \\ \| |\Phi, M'_{a|x}\rangle\langle\Phi, M'_{a|x}| - |\mathrm{junk}\rangle\left(\mathbb{1}^{\mathrm{C}} \otimes M_{a|x}\right)|\psi\rangle\langle\mathrm{junk}|\langle\psi|\left(\mathbb{1}^{\mathrm{C}} \otimes M_{a|x}\right)\|_1 &\leq f(\varepsilon) \end{aligned}$$

for $|\Phi\rangle = \Phi(|\psi\rangle)$, $|\Phi, M'_{a|x}\rangle = \Phi(\mathbb{1}^{\mathrm{C}} \otimes M'_{a|x}|\psi'\rangle)$, $|\mathrm{junk}\rangle \in \mathscr{H}^{\mathrm{P}}$ and $f : \mathbb{R} \to \mathbb{R}$.

Instead of directly bounding the distance between reference and physical probabilities, we can indirectly bound this distance by utilising an steering inequality. In the literature on standard self-testing, probability distributions that near-maximally violate a Bell inequality robustly self-test the state and measurements that produce the maximal violation [MYS14, RUV13, Kan16]. As a first requirement, there needs to be a unique probability distribution that achieves this maximal violation, and we now have many examples of Bell inequalities where this happens. The same applies to steering inequalities: there needs to be a unique assemblage that produces the maximal violation of a steering inequality. Furthermore this unique assemblage needs to imply a unique reference experiment (up to a local isometry). For steering inequalities of the form $\sum_{a|x} \alpha_{a,x} \mathrm{tr}\left(N_{a|b}\sigma'_{a|x}\right) \leq 0$ for real numbers $\alpha_{a,x}$, any assemblage that violates this inequality necessarily demonstrates steering. If all quantum assemblages satisfy $\sum_{a|x} \alpha_{a,x} \mathrm{tr}\left(F_{a|b}\sigma_{a|x}\right) \leq \beta$ for some positive real number β then β is the maximal violation of the steering inequality. If we consider probabilities of the form $p'(a,b|x,y) = \mathrm{tr}\left(N_{b|y}\sigma'_{a|x}\right)$ that satisfy $\sum_{a|x} \alpha_{a,x} \mathrm{tr}\left(N_{a|b}\sigma'_{a|x}\right) \geq (\beta - \varepsilon)$ then they are at most ε-far from the reference experiment that produces the maximal violation of $-\beta$. We will make use of this approach to CST in Sec. 5.5.2.

As explained in Section 2.5 an important issue in standard self-testing is that experimental probabilities are invariant upon taking the complex conjugate of both the state and measurements, which is not a physical operation. In this sense , the AST approach is advantageous to the standard self-testing approach in that we can rule out the state and measurements in the reference experiment both being the complex conjugate of our ideal reference experiment. This is because the assemblage is not invariant with respect to the complex conjugation. In this respect CST inherits problems from the standard self-testing if the measurements performed by the client are invariant under complex conjugation. In that case the provider can prepare a state and make measurements that are both the complex conjugate of the ideal case without altering the statistics. This can be remedied by the client choosing measurements that have complex entries as long as it does not drastically affect the ability to achieve $f(\varepsilon)$-CST.

5.5 Self-testing of a maximally entangled pair of qubits

In this section we discuss the possibilities to self-test the emblematic state of quantum information, the maximally entangled pair of qubits (or, *ebit*). Nowadays there is an extensive literature on standard self-testing of an ebit. The most compact self-test relies on the maximal violation of the CHSH inequality (see Sec. 2.5.2). The result is robust, meaning that a violation of $2\sqrt{2} - \varepsilon$ necessarily comes from states that are $O(\sqrt{\varepsilon})$-close to the ebit (up to local isometries). We turn to AST and CST to see if we can improve the current approaches from the standard self-testing when it comes to robustness. In particular, in Sec. 5.5.1 we use analytical approaches for AST and show that, for the ebit, $O(\sqrt{\varepsilon})$-AST is possible with a reasonable constant in front of the $\sqrt{\varepsilon}$. In Sec. 5.5.2 we exploit numerical methods for CST where the study of probabilities instead of assemblages is currently more amenable. We show that $O(\sqrt{\varepsilon})$-CST is possible and also that our numerical methods do better than existing numerical methods for the standard self-testing. Thirdly, in Sec. 5.5.3 we show that $O(\sqrt{\varepsilon})$-AST is essentially the best that one can hope for by explicitly giving a physical state and measurements where $f(\varepsilon)$ in the definition of $f(\varepsilon)$-AST will be at least $\sqrt{\varepsilon}$. In other words, $O(\varepsilon)$-AST is impossible.

5.5.1 Analytical results utilising the SWAP isometry

At this point let us define the reference experiment that will be the main aim of this section. The reference state and measurements are

$$\begin{aligned} |\psi\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \\ M_{0|0} = |0\rangle\langle 0|, \quad M_{1|0} = |1\rangle\langle 1|, \\ M_{0|1} = |+\rangle\langle +|, \quad M_{1|1} = |-\rangle\langle -|, \end{aligned}$$

where we have dropped the system labels for clarity. The assemblage corresponding to this reference experiment has the following elements:

$$\begin{aligned} \sigma_{0|0} &= \frac{1}{2}|0\rangle\langle 0|, & \sigma_{1|0} &= \frac{1}{2}|1\rangle\langle 1|, \\ \sigma_{0|1} &= \frac{1}{2}|+\rangle\langle +|, & \sigma_{1|1} &= \frac{1}{2}|-\rangle\langle -|. \end{aligned}$$

For this reference experiment we will use name *EPR experiment*. We are now ready to state the main result about AST for this experiment.

Theorem 9. *For the EPR experiment, $f(\varepsilon)$-robust assemblage-based one-sided self-testing is possible for $f(\varepsilon) = 24\sqrt{\varepsilon} + \varepsilon$.*

Before proving this theorem we will present two useful observations that will be used in the proof. The first observation is a lemma about the norm that we are using while the second is specific to the self-testing of the EPR experiment. We require the notation $\| |v\rangle \| = \sqrt{\langle v|v\rangle}$.

Lemma 9.1. *For any two vectors $|u\rangle$, $|v\rangle$ where $\||u\rangle\| \leq 1$ and $\||v\rangle\| \leq 1$, if $\| |u\rangle - |v\rangle \| \leq \eta \leq 1$, then for another vector $|t\rangle$ such that $\||t\rangle\| \leq \beta$, $\|(|u\rangle - |v\rangle)\langle t|\|_1 \leq \beta\eta$ and $\| |t\rangle(\langle u| - \langle v|)\|_1 \leq \beta\eta$*

Proof. This fact essentially follows from the definition of $\|\cdot\|$. That is, $\| |u\rangle - |v\rangle \| = \sqrt{\langle u|u\rangle + \langle v|v\rangle - \langle u|v\rangle - \langle v|u\rangle}$ and since the rank of $B = (|u\rangle - |v\rangle)\langle t|$ is 1 then the $\|B\|_1 = \sqrt{\mathrm{tr}(BB^\dagger)} = \| |t\rangle \| \sqrt{\langle u|u\rangle + \langle v|v\rangle - \langle u|v\rangle - \langle v|u\rangle}$ which, along with the fact that $\|B\|_1 = \|B^\dagger\|_1$, concludes our proof. □

The next observation follows directly from the definition of $f(\varepsilon)$-AST:

Lemma 9.2. *If $\|\sigma'_{a|x} - \sigma_{a|x}\|_1 \leq \varepsilon$ and $D(\rho'^{\mathrm{C}}, \rho^{\mathrm{C}}) \leq \varepsilon$ then*

$$\|\mathbb{1}^{\mathrm{C}} \otimes M'_{a|x}|\psi'\rangle - M_{a|x} \otimes \mathbb{1}^{\mathrm{P}}|\psi'\rangle\| \leq 2\sqrt{\varepsilon}$$

Proof. The proof follows from a series of basic observations:

$$
\begin{aligned}
&\| \mathbb{1}^{\mathrm{C}} \otimes M'_{a|x} \, |\psi'\rangle - M_{a|x} \otimes \mathbb{1}^{\mathrm{P}} \, |\psi'\rangle \, \| = \\
&\qquad = \sqrt{\langle\psi'| \, \mathbb{1}^{\mathrm{C}} \otimes M'_{a|x} \, |\psi'\rangle + \langle\psi'| M_{a|x} \otimes \mathbb{1}^{\mathrm{P}} \, |\psi'\rangle - 2 \, \langle\psi'| M_{a|x} \otimes M'_{a|x} \, |\psi'\rangle} \\
&\qquad \leq \sqrt{1 + 2\varepsilon - 2 \, \langle\psi'| M_{a|x} \otimes M'_{a|x} \, |\psi'\rangle} \\
&\qquad \leq \sqrt{1 + 2\varepsilon - 2(\frac{1}{2} - \varepsilon)} \\
&\qquad = 2\sqrt{\varepsilon}.
\end{aligned}
$$

The first inequality results from the fact that $\langle\psi'| \, \mathbb{1}^{\mathrm{C}} \otimes M'_{a|x} \, |\psi'\rangle = \mathrm{tr}_{\mathrm{P}}\left(\sigma'_{a|x}\right)$ and $\langle\psi'| M_{a|x} \otimes \mathbb{1}^{\mathrm{P}} \, |\psi'\rangle = \mathrm{tr}_{\mathrm{P}}(M_{a|x}\rho'^{\mathrm{C}})$ and that $|\mathrm{tr}(\sigma'_{a|x} - \sigma_{a|x})| \leq \varepsilon$ and $|\mathrm{tr}(M_{a|x}\rho'^{\mathrm{C}} - M_{a|x}\rho^{\mathrm{C}})| \leq \varepsilon$. The second inequality follows from the observation that $|\mathrm{tr}(M_{a|x}\sigma'_{a|x} - M_{a|x}\sigma_{a|x})| \leq \varepsilon$. □

We are now in a position to prove Theorem 9.

Proof. Recall that we are promised that

$$
\begin{aligned}
D(\rho'^{\mathrm{C}}, \rho_{\mathrm{C}}) &\leq \varepsilon, \\
\|\sigma'_{a|x} - \sigma_{a|x}\|_1 &\leq \varepsilon,
\end{aligned}
$$

for all a, x where $\rho^{\mathrm{C}} = \mathrm{tr}_{\mathrm{P}}\left(|\psi\rangle\langle\psi|\right)$. The aim is now to find an explicit isometry Φ that gives a non-trivial upper bound for the following expression:

$$
\| \, |\Phi, Q'_{a|x}\rangle \langle\Phi, Q'_{a|x}| - |\mathrm{junk}\rangle \langle\mathrm{junk}| \otimes (\mathbb{1}^{\mathrm{C}} \otimes Q_{a|x}) \, |\psi\rangle \langle\psi| \, (\mathbb{1}^{\mathrm{C}} \otimes Q_{a|x}) \|_1, \tag{5.4}
$$

for $Q'_{a|x} \in \{\mathbb{1}, M'_{a|x}\}$, $Q_{a|x} \in \{\mathbb{1}, M_{a|x}\}$ and $|\Phi, Q'_{a|x}\rangle$ as defined before. We first focus on the cases where $Q'_{a|x} = \mathbb{1}^{\mathrm{P}}$ and $Q_{a|x} = \mathbb{1}^{\mathrm{P}}$ and use this to argue the more general result.

The isometry that we use is the so-called SWAP isometry that has already been introduced in Chapter sec:chainST. Here we use the variant of the isometry apt for the steering scenario. In this isometry (see Fig. 5.2) an ancilla qubit is introduced in the state $|+\rangle^{\mathrm{P}'} \in \mathscr{H}^{\mathrm{P}'}$ where P' denotes the ancilla register on the provider's side in addition to the provider's Hilbert space $\mathscr{H}^{\mathrm{P}}$. After introducing the ancilla a unitary operator is applied to both the provider's part of the physical state and the ancilla, i.e. $|\psi'\rangle \, |+\rangle^{\mathrm{P}'} \to (\mathbb{1}^{\mathrm{C}} \otimes VHU) \, |\psi'\rangle \, |+\rangle \, \mathrm{P}'$ where $U = |0\rangle\langle 0|^{\mathrm{P}'} \otimes \mathbb{1}^{\mathrm{P}} + |1\rangle\langle 1|^{\mathrm{P}'} \otimes Z^{\mathrm{P}}$, $V = |0\rangle\langle 0|^{\mathrm{P}'} \otimes \mathbb{1}^{\mathrm{P}} + |1\rangle\langle 1|^{\mathrm{P}'} \otimes X^{\mathrm{P}}$ and $H = |+\rangle\langle 0| + |-\rangle\langle 1|$ and $Z = 2M'_{0|0} - \mathbb{1}^{\mathrm{P}}$, $X = 2M'_{0|1} - \mathbb{1}^{\mathrm{P}}$ and $X^2 = Z^2 = \mathbb{1}^{\mathrm{P}}$. After applying this isometry to the physical state $|\psi'\rangle$ we obtain the state

$$
M'_{0|0} \, |\psi'\rangle \, |0\rangle^{\mathrm{P}'} + XM'_{1|0} \, |\psi'\rangle \, |1\rangle^{\mathrm{P}'}.
$$

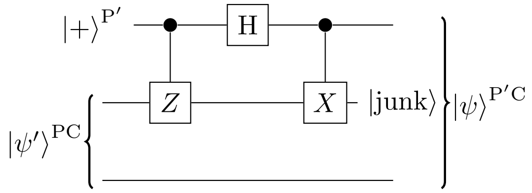
$|+\rangle^{\mathrm{P}'}$
H
Z
X
$|\psi'\rangle^{\mathrm{PC}}$
$|\mathrm{junk}\rangle$
$|\psi\rangle^{\mathrm{P'C}}$

Figure 5.2: For readers' convenience we give the figure of the SWAP gate suitable for the steering scenario. It is the special case of the standard SWAP gate represented on Fig. 3.1. In case the provider is applying the anticommuting measurement observables the circuit will transfer providers state to the ancillary qubit initiated in the state $|+\rangle$.

Therefore we wish to give an upper bound to

$$\| |\Xi\rangle \langle Xi| - |\mathrm{junk}\rangle \langle \mathrm{junk}| \otimes |\psi\rangle \langle \psi| \|_1 . \tag{5.5}$$

where

$$|\Xi\rangle = (M'_{0|0} |\psi'\rangle) |0\rangle^{\mathrm{P}'} + (XM'_{1|0} |\psi'\rangle) |1\rangle^{\mathrm{P}'}$$

At this point we can now apply a combination of Lemma 9.1 and Lemma 9.2 to bound this norm. Firstly, we observe that by virtue of Lemma 9.2 we have that

$$\left\| \left((M'_{0|0} |\psi'\rangle) |0\rangle^{\mathrm{P}'} + (XM'_{1|0} |\psi'\rangle) |1\rangle^{\mathrm{P}'} \right) - \left((M_{0|0} |\psi'\rangle) |0\rangle^{\mathrm{P}'} + (XM'_{1|0} |\psi'\rangle) |1\rangle^{\mathrm{P}'} \right) \right\| \leq 2\sqrt{\varepsilon},$$
$$\left\| \left((M_{0|0} |\psi'\rangle) |0\rangle^{\mathrm{P}'} + (XM'_{1|0} |\psi'\rangle) |1\rangle^{\mathrm{P}'} \right) - \left((M_{0|0} |\psi'\rangle) |0\rangle^{\mathrm{P}'} + (M_{1|0} \otimes X |\psi'\rangle) |1\rangle^{\mathrm{P}'} \right) \right\| \leq 2\sqrt{\varepsilon},$$

where, for the sake of brevity, we do not write identities $\mathbb{1}^{\mathrm{C}}$, e.g. $M'_{0|0} |\psi'\rangle = \mathbb{1}^{\mathrm{C}} \otimes M'_{0|0} |\psi'\rangle$.

We can apply these observations in conjunction with Lemma 9.1 (and noticing that $\| (M'_{0|0} |\psi'\rangle) |0\rangle^{\mathrm{P}'} + (XM'_{1|0} |\psi'\rangle) |1\rangle^{\mathrm{P}'} \| = 1$) to Eq. 5.5 to obtain

$$\begin{aligned}
&\left\| \left(M'_{0|0} |\psi'\rangle |0\rangle^{\mathrm{P}'} + XM'_{1|0} |\psi'\rangle |1\rangle^{\mathrm{P}'} \right) \left(\langle \psi' | M'_{0|0} \langle 0|^{\mathrm{P}'} + \langle \psi' | M'_{1|0} X \langle 1|^{\mathrm{P}'} \right) - J \otimes \Psi \right\|_1 \\
&\leq 2\sqrt{\varepsilon} + \left\| \left(M_{0|0} |\psi'\rangle |0\rangle^{\mathrm{P}'} + XM'_{1|0} |\psi'\rangle |1\rangle^{\mathrm{P}'} \right) \left(\langle \psi' | M'_{0|0} \langle 0|^{\mathrm{P}'} + \langle \psi' | M'_{1|0} X \langle 1|^{\mathrm{P}'} \right) - J \otimes \Psi \right\|_1 \\
&\leq 4\sqrt{\varepsilon} + \left\| \left(M_{0|0} |\psi'\rangle |0\rangle^{\mathrm{P}'} + M'_{1|0} X |\psi'\rangle |1\rangle^{\mathrm{P}'} \right) \left(\langle \psi' | M'_{0|0} \langle 0|^{\mathrm{P}'} + \langle \psi' | M'_{1|0} X \langle 1|^{\mathrm{P}'} \right) - J \otimes \Psi \right\|_1 ,
\end{aligned}$$

where $J = |\mathrm{junk}\rangle \langle \mathrm{junk}|$ and $\Psi = |\psi\rangle \langle \psi|$. Since $X = 2M'_{0|1} - \mathbb{1}$ and, for the Pauli-X matrix $\sigma_{\mathrm{X}} = 2 |+\rangle \langle +| - \mathbb{1}$, we obtain

$$\| \mathbb{1}^{\mathrm{C}} \otimes X^{\mathrm{P}} |\psi'\rangle - \sigma_{\mathrm{X}}^{\mathrm{C}} \otimes \mathbb{1}^{\mathrm{P}} |\psi'\rangle \| \leq 2 \| \mathbb{1}^{\mathrm{C}} \otimes {M'_{0|1}}^{\mathrm{P}} |\psi'\rangle - M_{0|1}^{\mathrm{C}} \otimes \mathbb{1}^{\mathrm{P}} |\psi'\rangle \| - \| |\psi'\rangle - |\psi'\rangle \| \leq 4\sqrt{\varepsilon}.$$

This further implies

$$\begin{aligned}&\left\|\left(M'_{0|0}\left|\psi'\right\rangle\left|0\right\rangle^{\mathrm{P}'}+XM'_{1|0}\left|\psi'\right\rangle\left|1\right\rangle^{\mathrm{P}'}\right)\left(\left\langle\psi'\right|M'_{0|0}\left\langle 0\right|^{\mathrm{P}'}+\left\langle\psi'\right|M'_{1|0}X\left\langle 1\right|^{\mathrm{P}'}\right)-J\otimes\Psi\right\|_1\\&\leq 8\sqrt{\varepsilon}+\left\|\left(E_{0|0}\left|\psi\right\rangle\left|0\right\rangle^{\mathrm{P}'}+M_{1|0}X\left|\psi\right\rangle\left|1\right\rangle^{P'}\right)\left(\left\langle\psi\right|E_{0|0}\left\langle 0\right|^{\mathrm{P}'}+\left\langle\psi'\right|M'_{1|0}X\left\langle 1\right|^{\mathrm{P}'}\right)-J\otimes\Psi\right\|_1.\end{aligned}$$

We will now apply the same reasoning to $\left(\left\langle\psi'\right|M'_{0|0}\left\langle 0\right|^{\mathrm{P}'}+\left\langle\psi'\right|M'_{1|0}X\left\langle 1\right|^{\mathrm{P}'}\right)$ but we need the fact that

$$\left\|M_{0|0}\left|\psi'\right\rangle\left|0\right\rangle^{\mathrm{P}'}+M_{1|0}\sigma_{\mathrm{X}}\left|\psi'\right\rangle\left|1\right\rangle^{\mathrm{P}'}\right\|=\sqrt{2\left\langle\psi'\right|M_{0|0}\left|\psi'\right\rangle}\leq\sqrt{1+2\varepsilon}\leq 1+\varepsilon,$$

which follows from the condition on the reduced state ρ'^{C} and $M_{1|0}\sigma_{\mathrm{X}}=\sigma_{\mathrm{X}}M_{0|0}$. Using these observations and Lemma 9.2 we arrive at

$$\begin{aligned}&\left\|\left(M'_{0|0}\left|\psi'\right\rangle\left|0\right\rangle^{\mathrm{P}'}+XM'_{1|0}\left|\psi'\right\rangle\left|1\right\rangle^{\mathrm{P}'}\right)\left(\left\langle\psi'\right|M'_{0|0}\left\langle 0\right|^{\mathrm{P}'}+\left\langle\psi'\right|M'_{1|0}X\left\langle 1\right|^{\mathrm{P}'}\right)-J\otimes\Psi\right\|_1\\&\leq 16\sqrt{\varepsilon}+8\varepsilon\sqrt{\varepsilon}\\&+\left\|\left(M_{0|0}\left|\psi'\right\rangle\left|0\right\rangle^{\mathrm{P}'}+M_{1|0}\sigma_{\mathrm{X}}\left|\psi'\right\rangle\left|1\right\rangle^{\mathrm{P}'}\right)\left(\left\langle\psi'\right|M_{0|0}\left\langle 0\right|^{\mathrm{P}'}+\left\langle\psi'\right|\sigma_{\mathrm{X}}M_{1|0}\left\langle 1\right|^{\mathrm{P}'}\right)-J\otimes\Psi\right\|_1\\&=16\sqrt{\varepsilon}+8\varepsilon\sqrt{\varepsilon}\\&+\left\|\left(\langle 0^{\mathrm{C}}\left|\psi'\right\rangle\left|00\right\rangle^{\mathrm{CP}'}+\langle 0^{\mathrm{C}}\left|\psi'\right\rangle\left|11\right\rangle^{\mathrm{CP}'}\right)\left(\left\langle\psi'\right|0\rangle^{\mathrm{C}}\left\langle 00\right|^{\mathrm{CP}'}+\left\langle\psi'\right|0\rangle^{\mathrm{C}}\left\langle 11\right|^{\mathrm{CP}'}\right)-J\otimes\Psi\right\|_1\\&=16\sqrt{\varepsilon}+8\varepsilon\sqrt{\varepsilon}+\left\|2\langle 0^{\mathrm{C}}\left|\psi'\right\rangle\left|\psi\right\rangle\left\langle\psi'\right|0\rangle^{\mathrm{C}}\left\langle\psi\right|-J\otimes\Psi\right\|_1\\&\leq 16\sqrt{\varepsilon}+8\varepsilon\sqrt{\varepsilon}+\left\|2\langle 0^{\mathrm{C}}\left|\psi'\right\rangle\left\langle\psi'\right|0\rangle^{\mathrm{C}}-J\right\|_1\\&\leq 16\sqrt{\varepsilon}+8\varepsilon\sqrt{\varepsilon}+2\varepsilon,\end{aligned}$$

where to obtain the last inequality we chose $\left|\mathrm{junk}\right\rangle$ to be the pure state that is proportional to $\left|0\right\rangle^{\mathrm{C}}\langle 0^{\mathrm{C}}\left|\psi'\right\rangle$, i.e. $\left|\mathrm{junk}\right\rangle=\beta^{-\frac{1}{2}}\left|0\right\rangle^{\mathrm{C}}\langle 0^{\mathrm{C}}\left|\psi'\right\rangle$ where $\beta=\langle\psi'|0\rangle^{\mathrm{C}}\langle 0^{\mathrm{C}}|\psi\rangle$ thus $|\mathrm{tr}\left(|0\rangle^{\mathrm{C}}\langle 0^{\mathrm{C}}|\rho'^{\mathrm{C}}\right)-\mathrm{tr}\left(|0\rangle^{\mathrm{C}}\langle 0^{\mathrm{C}}|\rho^{\mathrm{C}}\right)|\leq|\beta-\frac{1}{2}|\leq\varepsilon$.

We have shown that $D(\left|\Phi\right\rangle\left\langle\Phi\right|,\left|\mathrm{junk}\right\rangle\left\langle\mathrm{junk}\right|\otimes\left|\psi\right\rangle\left\langle\psi\right|)\leq 8\sqrt{\varepsilon}+4\varepsilon\sqrt{\varepsilon}+\varepsilon$. Now we consider the case of self-testing where measurements are made. That is, establishing an upper bound on the expressions of the form in Eq. (5.4) where $Q'_{a|x}\neq\mathbb{1}^{\mathrm{P}}$ and $Q_{a|x}\neq\mathbb{1}$ and after applying the SWAP isometry described above, the projector acting on the physical state $M'_{a|x}\left|\psi'\right\rangle$ gets mapped to

$$M'_{0|0}M'_{a|x}\left|\psi'\right\rangle\left|0\right\rangle^{\mathrm{P}'}+XM'_{1|0}M'_{a|x}\left|\psi'\right\rangle\left|1\right\rangle^{\mathrm{P}'}.$$

In the case $x=0$, utilising the fact that $M'_{a|x}M'_{a'|x}=\delta^{a}_{a'}M'_{a|x}$, for Eq. (5.4) we obtain:

$$\left\|M'_{0|0}\left|\psi'\right\rangle\left\langle\psi'\right|M'_{0|0}\otimes\left|0\right\rangle\left\langle 0\right|^{\mathrm{P}'}-\frac{1}{2}\left|\mathrm{junk}\right\rangle\left\langle\mathrm{junk}\right|\otimes\left|00\right\rangle\left\langle 00\right|^{\mathrm{CP}'}\right\|_1\text{ for }a=0,$$

$$\left\|XM'_{1|0}\left|\psi'\right\rangle\left\langle\psi'\right|M'_{1|0}X\otimes\left|1\right\rangle\left\langle 1\right|^{\mathrm{P}'}-\frac{1}{2}\left|\mathrm{junk}\right\rangle\left\langle\mathrm{junk}\right|\otimes\left|11\right\rangle\left\langle 11\right|^{\mathrm{CP}'}\right\|_1\text{ for }a=1.$$

By using the same reasoning as above we obtain the bounds $4\sqrt{\varepsilon}+\varepsilon$ and $12\sqrt{\varepsilon}+\varepsilon$ for the $a=0$ and $a=1$ cases respectively. For the case that $x=1$, more work is required in bounding Eq. (5.4). However, again by repeatedly applying the observation in Lem. 9.2 we obtain the bound of

$$\left\| |\Phi, Q'_{a|x}\rangle \langle \Phi, Q'_{a|x}| - |\text{junk}\rangle \langle \text{junk}| \otimes (\mathbb{1}^{\mathrm{C}} \otimes Q_{a|x}) |\psi\rangle \langle \psi| (\mathbb{1}^{\mathrm{C}} \otimes Q_{a|x}) \right\|_1 \leq 24\sqrt{\varepsilon}+\varepsilon, \tag{5.6}$$

thus concluding the proof. □

Central to the proof of this theorem was Lemma 9.2, but it is worth noting that the minimal requirements for proving this lemma were bounds on the probabilities and not necessarily bounds on the elements of the assemblage. We utilized the fact that bounds on the probabilities are obtained from the elements of the assemblage, but if one only bounds the probabilities then our result still follows. We then obtain the following corollary.

Corollary 9.1. *For the EPR experiment, $f(\varepsilon)$-robust correlation-based one-sided self-testing is possible for $f(\varepsilon)=24\sqrt{\varepsilon}+\varepsilon$.*

The fact that the function $f(\varepsilon)$ in Thm. 9 and Cor. 9.1 are the same suggests at the sub-optimality of our analysis, since AST could utilize more information than CST.

It is now worth commenting on the function $f(\varepsilon)$ and contrasting it with results in the standard self-testing literature. In particular, we want to contrast this result with other analytical approaches.[1] This is quite difficult since the measure of closeness to the ideal case is measured in terms of closeness to maximal violation of a Bell inequality and not in terms of elements of an assemblage or individual probabilities. Here we give an indicative comparison between the approach presented here and the current literature. Firstly, McKague, Yang and Scarani developed means of robust self-testing where if the observed violation of the CHSH inequality is ε-close to the maximal violation then the state is $O(\varepsilon^{(1/4)})$-close to the ebit [MYS14]. This is a less favourable polynomial than our result which demonstrates $O(\sqrt{\varepsilon})$-closeness. On the other hand, the work of Reichardt, Unger and Vazirani [RUV13] does demonstrate $O(\sqrt{\varepsilon})$-closeness in the state again if ε-close to the maximal violation of the CHSH inequality. However, the constant factor in front of the $\sqrt{\varepsilon}$ term has been calculated in Ref. [BNSTY15] to be of the order 10^5 and our result is several orders of magnitude better. In various other works [MS12, BP15, ŠASA16] more general families of self-testing protocols also demonstrate $O(\sqrt{\varepsilon})$-closeness of the physical state to the ebit when the violation is ε-far from Tsirelson's bound. We must emphasize that our analysis could definitely be tightened at several stages to lower the constants in $f(\varepsilon)$ but EPR-steering already yields an improvement over analytical methods in standard self-testing.

[1] These results were published prior to the publication of the currently best analytical robustness self-testing methods in Ref. [Kan16]. Thus, we compare robustness bounds to those known at the time of publication of the results from this chapter. The application of methods from Ref. [Kan16] to AST and CST should be subject of future research.

5.5.2 Numerical results utilising the SWAP isometry

Numerical approaches proved to be very useful for obtaining optimal robustness in the standard self-testing scenario [YVBSN14, BNSTY15]. In this section we explore robustness bounds of the ebit self-testing through EPR-steering with the aid of SDP optimizations. For that purpose we will shift from AST to CST, since that method is more appropriate and makes the comparison with the standard self-testing easier. We will not be considering CST in the strict sense, since we will only seek to establish a bound on the trace distance between the physical and reference states (up to isometries).

We start as in the analytical considerations of the previous section: construct the same SWAP isometry, apply it to the physical state and upper bound the norm from Eq. (5.5). Since this is the trace distance between the pure states, $M'_{0|0}\,|\psi'\rangle\,|0\rangle^{\mathrm{P'}} + XM'_{1|0}\,|\psi'\rangle\,|1\rangle^{\mathrm{P'}}$ and $|\mathrm{junk}\rangle\,|\mathrm{junk}\rangle$, we have that [NC00]

$$\begin{aligned}\frac{1}{2}\left\|\left(M'_{0|0}\,|\psi'\rangle\,|0\rangle^{\mathrm{P'}} + XM'_{1|0}\,|\psi'\rangle\,|1\rangle^{\mathrm{P'}}\right)\left(\langle\psi'|\,M'_{0|0}\,\langle 0|^{\mathrm{P'}} + \langle\psi'|\,M'_{1|0}X\,\langle 1|^{\mathrm{P'}}\right) - J\otimes\Psi\right\|_1 \leq \\ \leq \sqrt{1-(F^*)^2}\end{aligned}$$

where $F^* = \max F$ such that

$$\begin{aligned}F &= \sqrt{\langle\mathrm{junk}|\,\langle\psi|\left(M'_{0|0}\,|\psi'\rangle\,|0\rangle^{\mathrm{P'}} + XM'_{1|0}\,|\psi'\rangle\,|1\rangle^{\mathrm{P'}}\right)\left(\langle\psi'|\,M'_{0|0}\,\langle 0|^{\mathrm{P'}} + \langle\psi'|\,M'_{1|0}X\,\langle 1|^{\mathrm{P'}}\right)|\mathrm{junk}\rangle\,|\psi\rangle} \\ &= \frac{1}{\sqrt{2}}\sqrt{\langle\mathrm{junk}|\left(\langle 0|^{\mathrm{C}} M'_{0|0}\,|\psi'\rangle + \langle 1|^{\mathrm{C}} XM'_{1|0}\,|\psi'\rangle\right)\left(\langle\psi'|\,M'_{0|0}\,|0\rangle^{\mathrm{C}} + \langle\psi'|\,M'_{1|0}X\,|1\rangle^{\mathrm{C}}\right)|\mathrm{junk}\rangle}.\end{aligned}$$

In a similar manner like in Refs. [YVBSN14, BNSTY15], instead of bounding the fidelity F, we wish to bound a related quantity G which is the *singlet fidelity*. For $|\psi\rangle^{\mathrm{CP'}} = \frac{1}{\sqrt{2}}\,(|00\rangle + |11\rangle)$, this quantity is defined as

$$\begin{aligned}G &= \langle\tilde{\psi}'|\,\mathrm{tr}_{\mathrm{P}}\left[\left(M'_{0|0}\,|\psi'\rangle\,|0\rangle^{\mathrm{P'}} + XM'_{1|0}\,|\psi'\rangle\,|1\rangle^{\mathrm{P'}}\right)\left(\langle\psi'|\,M'_{0|0}\,\langle 0|^{\mathrm{P'}} + \langle\psi'|\,M'_{1|0}X\,\langle 1|^{\mathrm{P'}}\right)\right]|\psi\rangle \\ &= \frac{1}{2}\Bigg(\,\langle 0|^{\mathrm{C}}\,\sigma'_{0|0}\,|0\rangle^{\mathrm{C}} + 2\,\langle 0|^{\mathrm{C}}\,(\sigma'_{0|1,0|0} - \sigma'_{0|0,0|1,0|0})\,|1\rangle^{\mathrm{C}} + \qquad (5.7) \\ + &\qquad 2\,\langle 1|^{\mathrm{C}}\,(\sigma'_{0|0,0|1} - \sigma'_{0|0,0|1,0|0})\,|0\rangle^{\mathrm{C}} + \langle 1|^{\mathrm{C}}\,(\rho'^{\mathrm{C}} - \sigma'_{0|0})\,|1^{\mathrm{C}}\rangle\,\Bigg)\end{aligned}$$

such that

$$\sigma'_{0|1,0|0} = {\sigma'}^{\dagger}_{0|0,0|1} = \mathrm{tr}_{\mathrm{P}}(M'_{0|1}M'_{0|0}\,|\psi'\rangle\,\langle\psi'|)$$

and

$$\sigma'_{0|0,0|1,0|0} = \mathrm{tr}_{\mathrm{P}}(M'_{0|0}M'_{0|1}M'_{0|0}\,|\psi'\rangle\,\langle\psi'|).$$

Fidelity F^* and singlet fidelity G are related through $(F^*)^2 \geq 2G-1$ as shown in Ref. [BNSTY15].

Having the expression for G the aim is to understand how to find its lower bound given some correlations. As outlined in Sec. 2.4, every Bell inequality reduces to the corresponding steering inequality when the trusted side uses the adequate measurements. Let us restate the steering inequality (2.23), obtained from the CHSH Bell inequality. For easier comparison of robustness bounds we will scale its maximal violation to be the same as the maximal violation of the CHSH inequality. If the client applies measurements leading to the maximal violation of the CHSH inequality, $\{(\sigma_Z \pm \sigma_X)/\sqrt{2}\}$, on the assemblage generated in the EPR experiment the CHSH expression, denoted by tr$S$, can be written as

$$\begin{aligned}
\mathrm{tr}S = \mathrm{tr}\frac{1}{\sqrt{2}}\Big(&(\sigma_Z+\sigma_X)(\sigma'_{0|0}-\sigma'_{1|0})+(\sigma_Z+\sigma_X)(\sigma'_{0|1}-\sigma'_{1|1})+\\
&+(\sigma_Z-\sigma_X)(\sigma'_{0|0}-\sigma'_{1|0})-(\sigma_Z-\sigma_X)(\sigma'_{0|1}-\sigma'_{1|1})\Big)\\
=&\ \mathrm{tr}\left(\sqrt{2}\sigma_Z(\sigma'_{0|0}-\sigma'_{1|0})+\sqrt{2}\sigma_X(\sigma'_{0|1}-\sigma'_{1|1})\right)\\
=&\ \mathrm{tr}\left(\sqrt{2}\sigma_Z(2\sigma'_{0|0}-\rho'^{\mathrm{C}})+\sqrt{2}\sigma_X(2\sigma'_{0|1}-\rho'^{\mathrm{C}})\right).
\end{aligned}$$

The maximal value of tr$S$ is the well known Tsirelson's bound $2\sqrt{2}$. For a near-maximal violation we, thus, impose the constraint tr$S \geq 2\sqrt{2}-\eta$.

Numerical minimising the singlet fidelity G given constraint tr$S \geq 2\sqrt{2}-\eta$ can be phrased as an SDP optimization:

$$\begin{aligned}
\min \quad & \mathrm{tr}(M^T\Gamma) = G \\
\text{s. t.} \quad & \Gamma \geq 0, \\
& \mathrm{tr}(N^T\Gamma) = \mathrm{tr}S \geq 2\sqrt{2}-\eta,
\end{aligned} \tag{5.8}$$

where

$$\Gamma = \begin{pmatrix}
\rho'^{\mathrm{C}} & \sigma'_{0|0} & \sigma'_{0|1} & \sigma'_{0|0,0|1} \\
\sigma'_{0|0} & \sigma'_{0|0} & \sigma'_{0|1,0|0} & \sigma'_{0|0,0|1,0|0} \\
\sigma'_{0|1} & \sigma'_{0|0,0|1} & \sigma'_{0|1} & \sigma'_{0|0,0|1} \\
\sigma'_{0|1,0|0} & \sigma'_{0|0,0|1,0|0} & \sigma'_{0|1,0|0} & \sigma'_{0|0,0|1,0|0}
\end{pmatrix},$$

and

$$M = \frac{1}{2}\begin{pmatrix}
W & \mathbf{0} & \mathbf{0} & Y \\
\mathbf{0} & \sigma_Z & \mathbf{0} & \mathbf{0} \\
\mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
Y^T & \mathbf{0} & \mathbf{0} & -2\sigma_X
\end{pmatrix}, \qquad N = 2\sqrt{2}\begin{pmatrix}
\frac{-\sigma_X-\sigma_Z}{2} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
\mathbf{0} & \sigma_Z & \mathbf{0} & \mathbf{0} \\
\mathbf{0} & \mathbf{0} & \sigma_X & \mathbf{0} \\
\mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0}
\end{pmatrix},$$

such that $W = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $Y = \left(\begin{smallmatrix} 0 & 0 \\ 2 & 0 \end{smallmatrix}\right)$ and $\mathbf{0}$ is a 2-by-2 matrix of all zeroes. We constrain Γ in the optimization to be positive semi-definite. This is because Γ is a Gramian matrix and all Gramian matrices are positive semi-definite. First observe that entries of Γ are of the form $\Gamma_{ij} = \langle i|^{\mathrm{C}} \sigma' |j\rangle^{\mathrm{C}}$ for $\sigma \in \{\rho'^{\mathrm{C}}, \sigma'_{0|0}, \sigma'_{0|1}, \sigma'_{0|1,0|0}, \sigma'_{0|0,0|1}, \sigma'_{0|0,0|1,0|0}\}$. By the cyclic property of the partial trace we can also write $\sigma' = \mathrm{tr}_{\mathrm{P}}(F|\psi'\rangle\langle\psi'|G^{\dagger})$ for F, $G \in \{\mathbb{1}_{\mathrm{P}}, M'_{0|0}, M'_{0|1}, M'_{0|1}M'_{0|0}\}$. We now note that

$$\begin{aligned}
\langle i|^{\mathrm{C}} \sigma |j\rangle^{\mathrm{C}} &= \sum_{|y\rangle \in \mathscr{H}^{\mathrm{P}}} \langle i|^{\mathrm{C}} \langle y| F |\psi'\rangle \langle\psi'| G^{\dagger} |y\rangle |j\rangle^{\mathrm{C}} \\
&= \left(\sum_{|y\rangle \in \mathscr{H}^{\mathrm{P}}} \langle i|^{\mathrm{C}} \langle y| F |\psi'\rangle \langle y| \right) \left(\sum_{|y'\rangle \in \mathscr{H}^{\mathrm{P}}} \langle\psi'| G^{\dagger} |y'\rangle |j^{\mathrm{C}}\rangle |y'\rangle \right) \\
&= \sum_{y} \alpha_y \langle y| \sum_{y'} \alpha^{*}_{y'} |y'\rangle \\
&= \langle u|v\rangle
\end{aligned}$$

where $\{|y\rangle\}$ is an orthonormal basis in $\mathscr{H}^{\mathrm{P}}$ such that $\langle y'|y\rangle = \delta^{y}_{y'}$ and $\alpha_y = \langle i|^{\mathrm{C}} \langle y| F |\psi'\rangle$ is some scalar. Since the elements of Γ are all the inner product of vectors associated with a row and column, $\Gamma = V^{\dagger}V$ where V has column vectors associated with the vectors v. Therefore, Γ is Gramian. This then makes the above optimization problem a completely valid problem for lower bounding G. We further note that matrix Γ represents the EPR-steering analogue of the moment matrix in the Navascués- Pironio-Acín (NPA) hierarchy [NPA07] which is useful for approximating the set of quantum correlations.

In Fig. 5.3 we plot the lower bound on G achieved through this method and then compare it to the value obtained through the method of Bancal *et al* in Ref. [BNSTY15]. In both cases the violation of the CHSH inequality is lower-bounded by $2\sqrt{2} - \eta$, and we clearly see that the lower-bound is more favourable for our optimization through EPR-steering as compared to full device-independence. For the case of EPR-steering we observed that the plot can be lower-bounded by the function $1 - \eta/\sqrt{2}$ whereas the plot for device-independence is lower-bounded by $1 - 5\eta/4$. Respectively, these functions give an upper bound on $D(|\Phi\rangle\langle\Phi|, |\mathrm{junk}\rangle\langle\mathrm{junk}| \otimes |\psi\rangle\langle\psi|)$ of $2^{\frac{1}{4}}\sqrt{\eta} \leq 1.19\sqrt{\eta}$ and $\sqrt{10}/2\sqrt{\eta} \leq 1.59\sqrt{\eta}$.

5.5.3 Optimality of the SWAP isometry

The swap isometry showed to be useful in both, analytical and numerical approaches to self-testing in the EPR-steering scenario. While its simplicity allowed for clear demonstrations that self-testing is possible, the question of its optimality naturally arises. In other words, is there an isometry which would give a different error-scaling, better than the $\sqrt{\varepsilon}$ in the function $f(\varepsilon)$ for $f(\varepsilon)$-AST? In Sec. 5.1.1 we gave a counterexample to

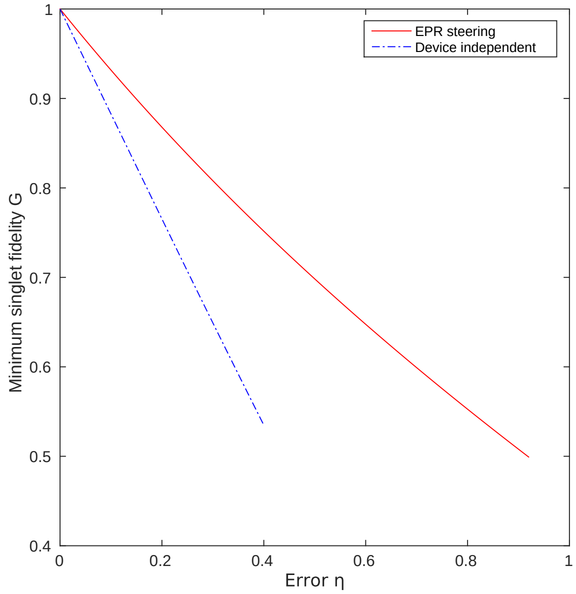

Figure 5.3: A graph numerically comparing self-testing of the ebit in a device-independent manner to our method based on EPR-steering. The error η is the distance from the maximal violation of the CHSH inequality.

the claim that a better error scaling is possible. However, the example therein is a bit unnatural, because the Hilbert space of the client, who is supposed to self-test a two-qubits state, is three-dimensional. At this point we would like to ask the question of the optimal error scaling while fixing the dimension of the client's Hilbert space to be equal to 2. We show that this is not possible and the best we can hope for is the $O(\sqrt{\varepsilon})$-AST which we have already established.

Let us now show that the trace distance between the physical and reference states in the EPR experiment can be $O(\varepsilon)$ for some isometries. For the EPR experiment, let us consider the trace distance $D(|\Phi\rangle\langle\Phi|, |\text{junk}\rangle\langle\text{junk}|\otimes|\psi\rangle\langle\psi|)$ for all possible isometries Φ and not just the SWAP isometry. An isometry will take the physical state $|\psi'\rangle$ to $U|\psi'\rangle|\hat{0}\rangle$ by introducing ancillae $|\hat{0}\rangle$ and applying a unitary U to the physical state and ancillae. As discussed in Sec. 5.1.1, the trace distance is then $D(U(|\psi'\rangle\langle\psi'|\otimes|\hat{0}\rangle\langle\hat{0}|)U^\dagger, |\text{junk}\rangle\langle\text{junk}|\otimes|\psi\rangle\langle\psi|) = \sqrt{1-F^2}$ for $F = |\langle\text{junk}|\langle\psi|U|\psi'\rangle|\hat{0}\rangle|$. We write $|\psi'\rangle$ in terms of its Schmidt decomposition

$$|\psi'\rangle = \sqrt{\lambda}|u\rangle|v\rangle + \sqrt{1-\lambda}|u^\perp\rangle|v^\perp\rangle$$

for λ as some real number such that $0 \leq \lambda \leq 1$ and $\langle u^\perp|u\rangle = \langle v^\perp|v\rangle = 0$. Since $|u\rangle$ is a state of a qubit it may be written as $|u\rangle = \cos\frac{\theta_1}{2}|0\rangle + e^{i\theta_2}\sin\frac{\theta_1}{2}|1\rangle$. Given this, we obtain

$$F = \frac{1}{\sqrt{2}}\Bigg| \langle\text{junk}|\langle 0|\left(\sqrt{\lambda}\cos\frac{\theta_1}{2}|w\rangle + \sqrt{1-\lambda}e^{-i\theta_2}\sin\frac{\theta_1}{2}|w^\perp\rangle\right) + \\ + \langle\text{junk}|\langle 1|\left(\sqrt{\lambda}e^{i\theta_2}\sin\frac{\theta_1}{2}|w\rangle - \sqrt{1-\lambda}\cos\frac{\theta_1}{2}|w^\perp\rangle\right)\Bigg|,$$

where $|w\rangle = U|v\rangle|\hat{0}\rangle$ and $|w^\perp\rangle = U|v^\perp\rangle|\hat{0}\rangle$. We now maximize F for all isometries so as to obtain a lower bound on $D(|\Phi\rangle\langle\Phi|, |\text{junk}\rangle\langle\text{junk}|\otimes|\psi\rangle\langle\psi|)$. The value of F will be maximized when $|w\rangle$ and $|w^\perp\rangle$ is in the linear span of $\{|\text{junk}\rangle|0\rangle, |\text{junk}\rangle|1\rangle\}$. Therefore, $|w\rangle = \cos\frac{\theta_3}{2}|\text{junk}\rangle|0\rangle + e^{i\theta_4}\sin\frac{\theta_3}{2}|\text{junk}\rangle|1\rangle$ and F^* will be the maximum of

$$\frac{1}{\sqrt{2}}\Bigg|\left(\sqrt{\lambda}\cos\frac{\theta_1}{2}\cos\frac{\theta_3}{2} + \sqrt{1-\lambda}e^{-i(\theta_2+\theta_4)}\sin\frac{\theta_1}{2}\sin\frac{\theta_3}{2}\right) + \\ + \left(\sqrt{\lambda}e^{i(\theta_2+\theta_4)}\sin\frac{\theta_1}{2}\sin\frac{\theta_3}{2} + \sqrt{1-\lambda}\cos\frac{\theta_1}{2}\cos\frac{\theta_3}{2}\right)\Bigg|$$

which then implies that $F^* = (1/\sqrt{2})(\sqrt{\lambda} + \sqrt{1-\lambda})$. We now wish to put bounds on λ which can be easily attained since $\rho'^{\text{C}} = \lambda|u\rangle\langle u| + (1-\lambda)|u^\perp\rangle\langle u^\perp|$ and $\rho^{\text{C}} = \frac{1}{2}\mathbb{1}^{\text{C}} = \frac{1}{2}(|u\rangle\langle u| + |u^\perp\rangle\langle u^\perp|)$. If we assume that $D(\rho'^{\text{C}}, \rho^{\text{C}}) = \varepsilon$ then we have that $|\lambda - \frac{1}{2}| = \varepsilon$ and thus

$$F^* = \frac{1}{\sqrt{2}}\left(\sqrt{\frac{1}{2}+\varepsilon} + \sqrt{\frac{1}{2}-\varepsilon}\right) = 1 - \frac{1}{2}\varepsilon^2 - O(\varepsilon^3),$$

where in the last equation we take the Taylor series expansion of F^* and $O(\varepsilon^3)$ represents polynomials of degree 3 and higher. In conclusion, given ε-closeness of the reduced states, there is an isometry Φ such that $D(|\Phi\rangle\langle\Phi|, |\text{junk}\rangle\langle\text{junk}|\otimes|\psi\rangle\langle\psi|) \leq O(\varepsilon)$. This then demonstrates that our SWAP isometry is not optimal for demonstrating such closeness between physical and reference states. However, the optimal isometry will be dependent on the basis $\{|u\rangle, |u^\perp\rangle\}$ and thus more complicated than the SWAP isometry.

We emphasize that this trace distance between physical and reference states (condition given in the first line of Eq. (5.3)) only amounts to a part of the criteria for AST. The other part of the criteria (the second line of Eq. (5.3)) rules out many isometries that might give the optimal trace distance between physical and reference states only. With this in mind we want to bound the expression in Eq. (5.4) for all possible isometries given ε-closeness between the elements of the physical and reference assemblages. In particular, we give an example of a physical experiment where ε-closeness for the assemblages is satisfied but for all isometries, the smallest value of Eq. (5.4) is $O(\sqrt{\varepsilon})$.

Example 9.1. *The physical state is*

$$|\psi'\rangle^{\text{CPP}'} = \frac{1}{\sqrt{2}}\left(\sqrt{1-\varepsilon}|00\rangle + \sqrt{\varepsilon}|11\rangle\right)|0\rangle + \frac{1}{\sqrt{2}}\left(\sqrt{\varepsilon}|00\rangle + \sqrt{1-\varepsilon}|11\rangle\right)|1\rangle$$

where P *and* P′ *denote two qubits that the provider has in their possession, thus* $\rho'^{\mathrm{C}} = \frac{1}{2}\mathbb{1}^{\mathrm{C}}$. *The physical measurements are* $M'_{0|0} = \mathbb{1}^{\mathrm{P}} \otimes |0\rangle\langle 0|^{\mathrm{P}'}$, $M'_{1|0} = \mathbb{1}^{\mathrm{P}} \otimes |1\rangle\langle 1|^{\mathrm{P}'}$, $M'_{0|1} = |+\rangle\langle +|^{\mathrm{P}} \otimes |+\rangle\langle +|^{\mathrm{P}'} + |-\rangle\langle -|^{\mathrm{P}} \otimes |-\rangle\langle -|^{\mathrm{P}'}$ *and* $M'_{1|1} = |+\rangle\langle +|^{\mathrm{P}} \otimes |-\rangle\langle -|^{\mathrm{P}'} + |-\rangle\langle -|^{\mathrm{P}} \otimes |+\rangle\langle +|^{\mathrm{P}'}$. *These physical measurements on the state produce the following assemblage elements:*

$$\sigma'_{0|0} = \frac{(1-\varepsilon)}{2}|0\rangle\langle 0|^{\mathrm{C}} + \frac{\varepsilon}{2}|1\rangle\langle 1|^{\mathrm{C}}, \qquad \sigma'_{1|0} = \frac{(1-\varepsilon)}{2}|1\rangle\langle 1|^{\mathrm{C}} + \frac{\varepsilon}{2}|0\rangle\langle 0|^{\mathrm{C}},$$
$$\sigma'_{0|1} = \frac{1}{2}|+\rangle\langle +|^{\mathrm{C}}, \qquad \sigma'_{1|1} = \frac{1}{2}|-\rangle\langle -|^{\mathrm{C}}.$$

We see then that $D(\rho'^{\mathrm{C}}, \rho^{\mathrm{C}}) = 0$ *and* $\|\sigma'_{a|x} - \sigma_{a|x}\| \leq \varepsilon$ *for all a, x.*

We now show that $\left\| |\Phi, M'_{0|0}\rangle\langle \Phi, M'_{0|0}| - |\text{junk}\rangle\langle\text{junk}| \otimes M_{0|0}|\psi\rangle\langle\psi|M_{0|0} \right\|_1 \geq \sqrt{\varepsilon}$ *for all possible isometries* Φ. *By considering all possible isometries we have*

$$|\Phi, M'_{0|0}\rangle = UM'_{0|0}|\psi'\rangle|\hat{0}\rangle = \frac{1}{\sqrt{2}}U\left(\sqrt{1-\varepsilon}|00\rangle^{\mathrm{CP}} + \sqrt{\varepsilon}|11\rangle^{\mathrm{CP}}\right)|0\rangle^{\mathrm{P}'}|\hat{0}\rangle = \frac{1}{\sqrt{2}}|\varepsilon\rangle,$$

for $|\varepsilon\rangle = U\left(\sqrt{1-\varepsilon}|00\rangle^{\mathrm{CP}} + \sqrt{\varepsilon}|11\rangle^{\mathrm{C}\mathbb{P}}\right)|0\rangle^{\mathrm{P}'}|\hat{0}\rangle$ *and* U *being a unitary applied jointly to the provider's qubits and the ancillae* $|\hat{0}\rangle$. *This then allows us to observe that*

$$\left\| |\Phi, M'_{0|0}\rangle\langle \Phi, M'_{0|0}| - |\text{junk}\rangle\langle\text{junk}| \otimes M_{0|0}|\psi\rangle\langle\psi|M_{0|0} \right\|_1 =$$
$$= D(|\varepsilon\rangle\langle\varepsilon|, |\text{junk}\rangle\langle\text{junk}| \otimes |00\rangle\langle 00|) = \sqrt{1 - |\langle\varepsilon|\text{junk}\rangle|00\rangle|^2}.$$

We see that $|\langle\varepsilon|\text{junk}\rangle|00\rangle|^2 = (1-\varepsilon)|\langle\text{junk}|\langle 0|U|0\rangle|\hat{0}\rangle|^2$ *which achieves the maximal value of* $(1-\varepsilon)$. *Therefore* $\| |\Phi, M'_{0|0}\rangle\langle\Phi, M'_{0|0}| - |\text{junk}\rangle\langle\text{junk}| \otimes M_{0|0}|\psi\rangle\langle\psi|M_{0|0}\|_1 \geq \sqrt{\varepsilon}$ *for all possible isometries* Φ.

This example demonstrates that $O(\varepsilon)$-AST is impossible for the EPR experiment and our analytical results are essentially optimal (up to constants).

5.6 Self-testing multi-partite states

All results presented so for belong to the simple bipartite scenario. Multipartite states are useful for many tasks and it is of interest to understand how self-testing of such states behaves in semi-device-independent scenarios. In this section we give a brief indication of how to generalize our set-up to the consideration of multipartite states. In Sec. 5.6.1 we will discuss the self-testing of tripartite states and give initial numerical results demonstrating the richness of this scenario. We will briefly sketch in Sec. 5.6.2 how EPR-steering could prove useful in establishing a tensor product structure within the provider's Hilbert space.

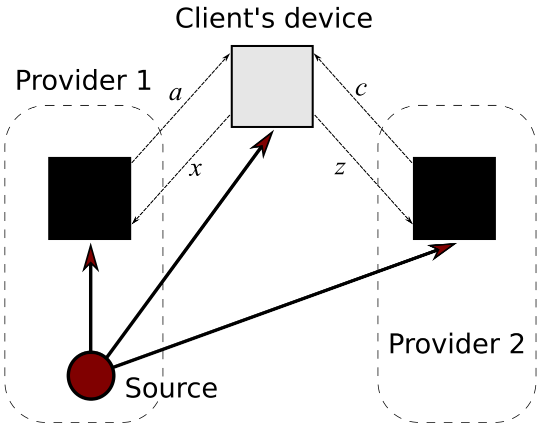

Figure 5.4: Here we depict the tripartite set-up with three parties where only one is the client, called the 1-trusted setting in the text. There are two non-communicating providers and we assume without loss of generality that one of them generates a quantum state and sends one part to the client and another to the other provider. The client may communicate with each provider individually and ask them to perform measurements.

5.6.1 Self-testing the GHZ state

There are several possible modifications of AST and CST set-ups when moving from the bipartite to the tripartite scenario. The first question is how to treat the third party, i.e. is it trusted or not? The simplest modifications is to make the additional party a trusted part of the client's laboratory. In that case the total Hilbert space of the client $\mathscr{H}^{\mathrm{C}}$ becomes the tensor product of the two Hilbert spaces associated with two trusted parties. Alternatively, as shown in Fig. 5.4, we can make the third party untrusted. They receive a share of the physical state via a quantum channel, but after that their communication via quantum channel with the initial provider stops. There are classical communication channels between both providers and the client. In this set-up the Hilbert spaces of two untrusted parties have a tensor product structure.

To illustrate the interesting differences between the bipartite and tri-partite cases, we look at the example of self-testing the Greenberger-Horne-Zeilinger (GHZ) state

$$|\psi\rangle = 1/\sqrt{2}\left(|\Phi^{-}\rangle^{1,2}|+\rangle^{3} + |\Psi^{+}\rangle^{1,2}|-\rangle^{3}\right)$$

where $|\Phi^{-}\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$ and $|\Psi^{+}\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$. In the scenario with two trusted parties (that together form the client), a qubit is sent from the provider to each of these parties (say, qubits 1 and 2 are sent); we will call this scenario the 2-*trusted setting*. In the other scenario with two non-communicating untrusted providers, a qubit (say, qubit 1) is sent to the client; we will call this scenario the 1-*trusted setting*. These different scenarios correspond to the different types of multipartite EPR-steering introduced in

Ref. [Cav+15].

We now describe the reference experiments for both settings for the state $|\psi\rangle$. In the case of the 2-trusted setting, as in the EPR experiment, the provider claims to make measurements $M_{j|0} = |j\rangle\langle j|$ for $j \in \{0,1\}$ as well as $M_{0|1} = |+\rangle\langle +|$ and $M_{1|1} = |-\rangle\langle -|$. The assemblage for the two trusted parties has elements

$$\sigma_{0|0} = \frac{1}{4}(|\Phi^-\rangle + |\Psi^+\rangle)(\langle\Psi^+| + \langle\Phi^-|), \qquad \sigma_{1|0} = \frac{1}{4}(|\Phi^-\rangle - |\Psi^+\rangle)(\langle\Phi^-| - \langle\Psi^+|),$$
$$\sigma_{0|1} = \frac{1}{2}|\Phi^-\rangle\langle\Phi^-|, \qquad \sigma_{1|1} = \frac{1}{2}|\Psi^+\rangle\langle\Psi^+|.$$

For the 1-trusted setting, in addition to the provider claiming to making the above measurements, the second untrusted party, or second provider claims also to make the same measurements, which we denote by $\bar{M}_{c|z}$ for $c,\ z \in \{0,1\}$. The assemblage will be $\{\sigma_{a,c|x,z}\}_{a,c,x,z}$ where each element is $\sigma_{a,c|x,z} = \mathrm{tr}_{\mathrm{P}}(\mathbb{1}^{\mathrm{C}} \otimes \bar{M}_{c|z} \otimes M_{a|x}|\psi\rangle\langle\psi|)$. The assemblage for the one trusted party will have 16 elements but for the sake of brevity we will not write out the elements.

We then wish to self-test this reference experiment when the elements of the physical assemblage are close to the elements of the ideal, reference experiment. Instead of doing this, we will mimic the numerical approach in Sec. 5.5.2 by considering the Mermin inequality (see Eq. (2.16)) adapted to the 1-trusted and 2-trusted scenarios. Utilising the notation of σ_{X} and σ_{Z} for the Pauli-X and Pauli-Z matrices respectively, for the 2-trusted and 1-trusted settings, the inequalities respectively are:

$$\begin{aligned}\mathrm{tr}B_2 =& 2\mathrm{tr}\Big((\sigma_{\mathrm{Z}}\otimes\sigma_{\mathrm{Z}})(2\sigma'_{0|1} - \rho'^{\mathrm{C}}) + (\sigma_{\mathrm{X}}\otimes\sigma_{\mathrm{Z}})(2\sigma'_{0|0} - \rho'^{\mathrm{C}}) + \\ &+ (\sigma_{\mathrm{Z}}\otimes\sigma_{\mathrm{X}})(2\sigma'_{0|0} - \rho'^{\mathrm{C}}) - (\sigma_{\mathrm{X}}\otimes\sigma_{\mathrm{X}})(2\sigma'_{0|1} - \rho'^{\mathrm{C}})\Big) \leq 2,\\ \mathrm{tr}B_1 =& 2\mathrm{tr}\left(\sigma_{\mathrm{Z}}(\sigma'_{00|01} - \sigma'_{01|01} - \sigma'_{10|01} + \sigma'_{11|01}) + \sigma_{\mathrm{X}}(\sigma'_{00|00} + \sigma'_{11|00} - \sigma'_{01|00} - \sigma'_{10|00})\right) + \\ & 2\mathrm{tr}\left(\sigma_{\mathrm{Z}}(\sigma'_{00|10} + \sigma'_{11|10} - \sigma'_{01|10} - \sigma'_{10|10}) - \sigma_{\mathrm{X}}(\sigma'_{00|11} + \sigma'_{11|11} - \sigma'_{01|11} - \sigma'_{10|11})\right) \leq 2.\end{aligned}$$

The maximal quantum violation of these inequalities is 4. We now aim to carry out self-testing if the physical experiment achieves a violation of $4-\eta$. For the untrusted parties, we implement the SWAP isometry to each of their systems as outlined in Sec. 5.5.1. For the 2-trusted setting, the physical state $|\psi'\rangle$ gets mapped to $|\psi_1\rangle = M'_{0|0}|\psi'\rangle|0\rangle^{\mathrm{P}'} + XM'_{1|0}|\psi'\rangle|1\rangle^{\mathrm{P}'}$. In the 1-trusted setting, the physical state $|\psi\rangle$ gets mapped to

$$\begin{aligned}|\psi_2\rangle = & M'_{0|0}\bar{M}'_{0|0}|\psi'\rangle|0\rangle^{\mathrm{P}'}|0\rangle^{\mathrm{P}''} + XM'_{1|0}\bar{M}'_{0|0}|\psi'\rangle|1\rangle^{\mathrm{P}'}|0\rangle^{\mathrm{P}''} + \\ & + M'_{0|0}\bar{X}\bar{M}'_{1|0}|\psi'\rangle|0\rangle^{\mathrm{P}'}|1\rangle^{\mathrm{P}''} + XM'_{1|0}\bar{X}\bar{M}'_{1|0}|\psi'\rangle|1\rangle^{\mathrm{P}'}|1\rangle^{\mathrm{P}''}\end{aligned}$$

where $\bar{M}'_{c|z}$ is the physical measurement made by the second untrusted party, $\bar{X} = 2\bar{M}'_{0|1} - \mathbb{1}$ and P' denotes the ancilla qubit introduced for one party and P'' for the other party.

Our figure of merit for closeness between the physical and reference states is the *GHZ fidelity* which for the 2-trusted and 1-trusted settings is G_2 and G_1 respectively where

$$\begin{aligned}G_2 &= \langle\psi|\,\mathrm{tr}_{\mathrm{P}}\left(|\psi_1\rangle\langle\psi_1|\right)|\psi\rangle\,,\\ G_1 &= \langle\psi|\,\mathrm{tr}_{\mathrm{P}}\left(|\psi_2\rangle\langle\psi_2|\right)|\psi\rangle\,,\end{aligned}$$

where in both cases we trace out the provider's (providers') Hilbert space(s) $\mathscr{H}^{\mathrm{P}}$. Now we minimize G_2 while $\mathrm{tr}B_2 \geq 4-\eta$ and minimize G_1 such that $\mathrm{tr}B_1 \geq 4-\eta$. These problems again can be lower-bounded by an SDP and in Fig. 5.5 we give numerical values obtained with these minimization problems. This case is numerically more expensive than the simple self-testing of the EPR experiment and for tackling it we used the SDP procedures described in Ref. [Wit15]. We also compare our results to those obtained in the device-independent setting where all three parties are not trusted but the violation of the GHZ-Mermin inequality is $4-\eta$. We see that the GHZ fidelity increases when we trust more parties. Interestingly, we can see that the curve for 1-trusted scenario is obviously closer to the curve of 2-trusted scenario than to the device-independent one. This may hint that multi-partite EPR-steering behaves quite differently to quantum non-locality. However, to draw this conclusion from self-testing one would have to pursue more rigorous research, since we have only obtained numerical lower bounds on the GHZ fidelity using only one specific isometry.

5.6.2 Establishing a tensor product structure

Another well-researched task in the standard self-testing literature is the certification of the existence of a tensor product of N EPR-pairs shared between two parties. The first work, proving this self-testing result in the scenario when parties make sequential, i.e. one after another, measurements on each EPR pair, was [RUV13]. Later the result was improved in the parallel scenario, when all the measurements are performed at the same time [Col17, McK17, CN16]. The main difficulty in these kinds of self-tests is to prove that the Hilbert spaces of the untrusted parties decompose as a tensor product of N two-dimensional Hilbert spaces: in each sub-space there is one-half of an ebit. The previous section hints that self-testing through EPR-steering could lead to a substantial improvement exactly in this scenario: establishing a tensor product structure in the provider's Hilbert space. A useful simplification EPR steering offers in this task is that in the client's laboratory a tensor product structure is known: the client knows they have, say, two qubits. If the assemblage for each qubit is close to the ideal case of being one half of an ebit, then we may use Lemma 9.2 to ”transfer” the providers's physical operations to one of the client's qubits. We also note that this observation forms part of the basis of the work

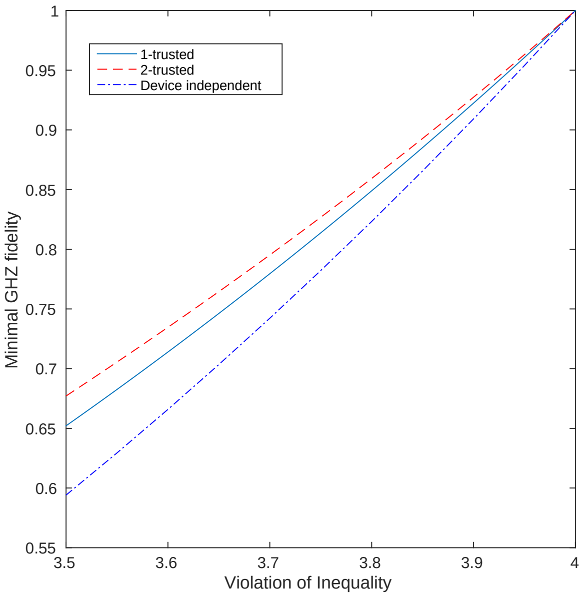

Figure 5.5: A graph numerically comparing the minimum GHZ fidelity for a given violation of the GHZ-Mermin inequality for different levels of trust in the devices. We observe that the line for the 1-trusted setting is closer to the 2-trusted setting than device-independence.

presented in Ref. [GWK17], in the context of verification of quantum computation.

More precisely, the client's Hilbert space is constructed from a tensor product of N two-dimensional Hilbert spaces, i.e. $\mathscr{H}^{\mathrm{C}} = \bigotimes_{i=1}^{N} \mathscr{H}^{\mathrm{C}_i}$ where $\mathscr{H}^{\mathrm{C}_i} = \mathbb{C}^2$. In this situation the reference state is $|\psi\rangle = \bigotimes_{i=1}^{N} |\psi_i\rangle \in \bigotimes_{i=1}^{N} \mathscr{H}^{\mathrm{P}_i} \otimes \mathscr{H}^{\mathrm{C}_i}$ for each $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathscr{H}^{\mathrm{P}_i} \otimes \mathscr{H}^{\mathrm{C}_i}$. On each Hilbert space $H^{\mathrm{P}i}$ acts a projective measurement $\{M_{a_i|x_i}\}$, where a_i, $x_i \in \{0,1\}$. Henceforth, the global reference projector is $\bigotimes_{i=1}^{N} M_{a_i|x_i}$ which acts on the Hilbert space $\bigotimes_{i=1}^{N} \mathscr{H}^{\mathrm{P}_i}$. Accordingly, the measurement choices and outputs are not bits, but bit-strings $\mathbf{x} := (x_1, x_2, ..., x_N)$ and $\mathbf{a} := (a_1, a_2, ..., a_N)$ respectively. We call this reference experiment the *N-pair EPR experiment* and we are now in a position to generalize Lemma 9.2.

Lemma 9.3. *For the N-pair EPR experiment, if for all i,* $\left\| \sigma'_{\boldsymbol{a}|\boldsymbol{x}} - \sigma_{\boldsymbol{a}|\boldsymbol{x}} \right\|_1 \leq \varepsilon$ *and* $D(\rho'^{\mathrm{C}}, \rho^{\mathrm{C}}) \leq \varepsilon$ *where* $\sigma_{\boldsymbol{a}|\boldsymbol{x}} = \bigotimes_{i=1}^{N} \sigma_{a_i|x_i}$ *and* $\rho^{\mathrm{C}} = \bigotimes_{i=1}^{N} \frac{\mathbb{1}^{\mathrm{C}}}{2}$ *then*

$$\left\| \mathbb{1}^{\mathrm{C}} \otimes M'_{\boldsymbol{a}|\boldsymbol{x}} |\psi'\rangle - \bigotimes_{i=1}^{N} M_{a_i|x_i} \otimes \mathbb{1}^{\mathrm{P}} |\psi'\rangle \right\| \leq 2\sqrt{\varepsilon}. \tag{5.9}$$

The proof of this lemma is completely equivalent to the proof of Lemma 9.2 so we will leave it out from our discussion. A nice relaxation of the conditions of the above lemma is to insist that each observed element of an assemblage $\sigma'_{a_i|x_i}$ is ε-close to $\sigma_{a_i|x_i}$ and still recover a similar result. This requires a little bit more work since we have not been specific about the model of the provider's measurements. For example, we have not stipulated whether the probability distribution $p(\mathbf{a}|\mathbf{x}) = \mathrm{tr}(\sigma'_{\mathbf{a}|\mathbf{x}})$ satisfies the no-signalling principle. Furthermore, even if these probabilities satisfy this principle, it does not immediately enforce a constraint on the behaviour of the measurements. For the sake of brevity we will not address this issue in this thesis.

5.7 Discussion

In this chapter we introduced and explored possibilities of self-testing based on EPR-steering. We have shown that the semi-device-independent scenario offers a broad range of tools useful for self-testing. By getting use of all the available resources one can perform quantum state tomography of a part of the state and use this information to develop better and simpler analytical methods. Alternatively, in some cases correlations of measurement outcomes of some fixed measurements with the outcomes of some untrused measurements is enough to obtain what is necessary for self-testing. Moreover, a near-maximal violation of an appropriate steering inequality can also suffice. After introducing different methods tailored for self-testing through EPR-steering we compared them to the standard device-independent approach and showed that EPR-steering simplifies proofs and gives more useful bounds for robustness. Hopefully, our approach could be used in future experiments where states produced are quite far from ideal but potentially useful for quantum information tasks. However, we note that EPR-steering-based self-testing substantially only improves the constants in the error terms (for robustness) and not the polynomial of the error, i.e. we can only demonstrate $O(\sqrt{\varepsilon})$-AST for the EPR experiment. This highlights that from the point-of-view of self-testing, EPR-steering behaves in the same way as Bell non-locality and not entanglement verification in which all parties are trusted.

One direction of research for the future work could be exploration of the self-testing of other quantum states, particularly non-maximally entangled states, such as partially entangled pairs of qubits. It is desirable to develop a general framework for self-testing many different states and measurements. This would be something akin to the work of Yang *et al* [YVBSN14] that utilizes the NPA hierarchy of SDPs. A related work by Kogias *et al* [KSCAA15] could prove useful in this aim. In addition to this, our work has hinted at the interesting possibilities for studying self-testing based on EPR-steering in the multipartite case. In future work we will investigate adapting our techniques to general multipartite states. For example, the general multipartite GHZ state can be self-testing by adapting the family of Bell inequalities found in Refs. [Ard92, BK93, HCLB11].

One may question our use of the Schatten 1-norm as a measure of distance between elements of a reference and physical assemblage. For example, the Schatten 2-norm is a lower bound on the 1-norm so could be a more useful measure of closeness. It may be worthwhile to explore this possibility but we note that the argument for the impossibility of $O(\varepsilon)$-AST for the EPR experiment in Section 5.5.3 still applies even if we replace all the distance measures with the 2-norm.

Finally, it would be interesting to consider relaxing the assumption of systems being independent and identically distributed (i.i.d) and tomography being performed in the asymptotic limit. This would take into account the provider having devices with memory as well as only being given a finite number of systems. In the case of CST, we may use statistical methods to bound the probability that the provider can deviate from their claims and trick us in accepting their claims. For the case of AST, tools from non-i.i.d. quantum information theory might be required which makes the future study of AST interesting from the point-of-view of quantum information.

Part II

Certification of different quantum resources and protocols

Chapter 6

Certifying and quantifying entanglement and randomness in quantum networks

The relation between Bell nonlocality and entanglement is one of the open questions in the foundations of quantum theory. While nonlocal correlations can only be obtained by performing local measurements on an entangled state, not every entangled state can lead to nonlocality. As it was first shown by Werner [Wer89] the probability distributions obtained by local measurements applied to certain entangled quantum states can be simulated by a purely classical model called a local-hidden-variable model. Werner's result was later generalized in many ways [Bar02, AGT06].

Since the standard Bell scenario exposes a gap between nonlocality and entanglement, one may ask if it is possible to come up with some alternative scenario in which every entangled state exhibits nonlocal correlations. One possibility is to make use of many copies of the shared entangled state. It has been proven that some entangled states which are not nonlocal in the standard Bell scenario can violate a Bell inequality in this scenario [Pal12, CABV13], a phenomenon known as super-activation. Whether every entangled state can be super-activated in this way is again an open problem. Another possibility is to consider a quantum network consisting of many copies of the same state shared among many parties [SBBZ05]. Similarly to superactivation, some states that are local in the standard Bell scenario become nonlocal in the network scenario. However, the general relation between entanglement and nonlocality is also unknown in this case. Another alternative Bell scenario, historically preceding the others, was suggested in Ref. [Pop95] and is known as the hidden nonlocality scenario. In it the parties are allowed to perform pre-processing on their shared state before applying their measurements. Even though some local entangled states can become nonlocal in this new scenario it has recently been shown that there are entangled states which can never exhibit hidden nonlocality, i.e. they remain nonlocal after arbitrary pre-processing [Hir+16]. Finally, it is possible to combine all the nonstandard Bell scenarios, but still there is no conclusive statement about the relation between entanglement and nonlocality in what would be called multy-copy with pre-processing scenario.

There is however one modification of the standard Bell scenario that can reveal nonlocal correlations from every entangled state. It consists of using measurement devices that receive quantum systems as inputs [Bus12] (See also Refs. [BRLG13, RBGL13, CHW13, Hal16] for further developments and Refs. [NMAB15, Xu+14, Ver+16] for experimental demonstrations). The observation of nonlocal correlations in this scenario can be seen as an entanglement test with uncharacterized measurement devices, which motivated the name of *measurement-device-independent nonlocality*.

In this chapter we shed new light on some aspects of this scenario with quantum inputs, explore its power for entanglement detection and quantification in quantum networks, and finally study its advantages for randomness certification.

6.1 Measurement-device-independent entanglement certification

We start this section by reviewing some of the main results on entanglement certification in Bell scenario with quantum inputs, and by proposing some improvements on this task. We consider two separated parties, Alice and Bob, sharing a bipartite system in an unknown state ρ^{AB} acting on the tensor product of Hilbert spaces $\mathscr{H}^{\mathrm{A}} \otimes \mathscr{H}^{\mathrm{B}}$. They want to certify if their system is entangled, but do not know how their measurement devices work. Buscemi proposed a solution to this problem [Bus12]: at each round of the experiment Alice and Bob encode their measurement choices in quantum states $\omega_x \in \mathscr{H}^{\mathrm{A}_0}$ and $\omega_y \in \mathscr{H}^{\mathrm{B}_0}$ respectively, which they use as inputs for their measurement devices. After receiving the quantum inputs the measurement devices provide classical outputs a and b according to the probability distributions

$$p(a,b|\omega_x,\omega_y) = \mathrm{Tr}[(M_a^{\mathrm{A}_0\mathrm{A}} \otimes M_b^{\mathrm{B}\mathrm{B}_0})(\omega_x^{\mathrm{A}_0} \otimes \rho^{\mathrm{AB}} \otimes \omega_y^{\mathrm{B}_0})], \tag{6.1}$$

where $M_a^{\mathrm{A}_0\mathrm{A}}$ and $M_b^{\mathrm{B}\mathrm{B}_0}$ are the measurement operators applied by the measurement devices on the corresponding input systems and their shares of state ρ^{AB}. Buscemi proved that if $\{\omega_{x/y}\}_{x/y}$ correspond to tomographically complete sets of input states [1] in $\mathscr{H}^{\mathrm{A/B}}$, and each box performs a Bell state measurement, then every entangled state ρ^{AB} produces

[1] By a tomographically complete set of input states we mean that the set is sufficient to perform quantum process tomography

a set of probability distributions $\{p(a,b|\omega_x,\omega_y)\}_{a,b,x,y}$ that cannot be reproduced with any separable state.

Building on this result, the authors of Ref. [BRLG13] provided a way to construct Bell tests with quantum inputs from every entanglement witness, and named them measurement-device-independent entanglement witnesses (MDIEW). However, when it comes to practical entanglement detection, MDIEW are useful only when one has a good guess on which entangled state should be detected, and can thus start from an entanglement witness which is able to detect its entanglement. In Ref. [Ver+16] a solution at the single copy level was given, by showing that the quantum inputs scenario can be cast as an SDP optimization problem, readily solvable with available software. We present here the said SDP in a slightly different form.

The starting point is the fact that the joint outcome probability distribution can be written in the following way

$$p(a,b|\omega_x,\omega_y) = \mathrm{Tr}[M_{a,b}^{\mathrm{A_0B_0}}(\omega_x^{\mathrm{A_0}} \otimes \omega_y^{\mathrm{B_0}})], \tag{6.2}$$

where $\tilde{M}_{a,b}$ is an effective POVM operator defined by

$$M_{a,b}^{\mathrm{A_0B_0}} = \mathrm{Tr_{AB}}[(M_a^{\mathrm{A_0A}} \otimes M_b^{\mathrm{BB_0}})(\mathbb{1}^{\mathrm{A_0}} \otimes \rho^{\mathrm{AB}} \otimes \mathbb{1}^{\mathrm{B_0}})]. \tag{6.3}$$

By construction, the effective POVM $M_{a,b}^{\mathrm{A_0B_0}}$ satisfies a number of conditions, which can be thought of as playing the role of ‘no-signalling’ conditions. In particular,

$$\sum_a M_{a,b}^{\mathrm{A_0B_0}} = \mathbb{1}^{\mathrm{A_0}} \otimes M_b^{\mathrm{B_0}} \qquad \sum_b M_{a,b}^{\mathrm{A_0B_0}} = M_a^{\mathrm{A_0}} \otimes \mathbb{1}^{\mathrm{B_0}} \tag{6.4}$$

where $M_b^{\mathrm{B_0}} \equiv \mathrm{tr_B}[M_b^{\mathrm{BB_0}}(\rho^{\mathrm{B}} \otimes \mathbb{1}^{\mathrm{B_0}})] \geq 0$ and $M_a^{\mathrm{A_0}} \equiv \mathrm{tr_A}[M_a^{\mathrm{AA_0}}(\mathbb{1}^{\mathrm{A_0}} \otimes \rho^{\mathrm{A}})] \geq 0$ are effective local POVMs for Alice and Bob (i.e. such that $\sum_a M_a^{\mathrm{A_0}} = \mathbb{1}^{\mathrm{A_0}}$ and $\sum_b M_b^{\mathrm{B_0}} = \mathbb{1}^{\mathrm{B_0}}$). We will write $\{M_{a,b}^{\mathrm{A_0B_0}}\}_{a,b} \in \mathscr{M}$ to denote the fact that the effective POVM satisfies these conditions, i.e.

$$\begin{aligned}\mathscr{M} = \Big\{ \{M_{a,b}^{\mathrm{A_0B_0}}\}_{a,b} | M_{a,b}^{\mathrm{A_0B_0}} \geq 0, \sum_a M_{a,b}^{\mathrm{A_0B_0}} = \mathbb{1}^{\mathrm{A_0}} \otimes M_b^{\mathrm{B_0}}, \\ \sum_b M_{a,b}^{\mathrm{A_0B_0}} = M_a^{\mathrm{A_0}} \otimes \mathbb{1}^{\mathrm{B_0}}, \sum_a M_a^{\mathrm{A_0}} = \mathbb{1}^{\mathrm{A_0}}, \sum_b M_b^{\mathrm{B_0}} = \mathbb{1}^{\mathrm{B_0}} \Big\}\end{aligned} \tag{6.5}$$

Now, if the shared state ρ^{AB} separable, *i.e.* $\rho^{\mathrm{AB}} = \sum_\lambda p_\lambda \rho_\lambda^{\mathrm{A}} \otimes \rho_\lambda^{\mathrm{B}}$, then Eq. (6.3) becomes

$$\begin{aligned}M_{a,b}^{\mathrm{A_0B_0}} &= \sum_\lambda p_\lambda \mathrm{Tr_A}[M_a^{\mathrm{A_0A}}(\mathbb{1}^{\mathrm{A_0}} \otimes \rho_\lambda^{\mathrm{A}})] \otimes \mathrm{Tr_B}[M_b^{\mathrm{BB_0}}(\rho_\lambda^{\mathrm{B}} \otimes \mathbb{1}^{\mathrm{B_0}})] \\ &= \sum_\lambda p_\lambda M_{a|\lambda}^{\mathrm{A_0}} \otimes M_{b|\lambda}^{\mathrm{B_0}}.\end{aligned} \tag{6.6}$$

where $M^{\mathrm{A_0}}_{a|\lambda} \equiv \mathrm{Tr}_{\mathrm{A}}[M^{\mathrm{A_0A}}_{a}(\mathbb{1}^{\mathrm{A_0}} \otimes \rho^{\mathrm{A}}_{\lambda})]$ and $M^{\mathrm{B_0}}_{b|\lambda} \equiv \mathrm{Tr}_{\mathrm{B}}[M^{\mathrm{BB_0}}_{b}(\rho^{\mathrm{B}}_{\lambda} \otimes \mathbb{1}^{\mathrm{B_0}})]$ are effective local POVMs for Alice and Bob. Consequently, the fact that ρ^{AB} is separable, implies that the operator $M^{\mathrm{A_0B_0}}_{a,b}$ is a separable operator for all a and b.

Alice and Bob can thus check the separability of ρ^{AB} by solving the following feasibility problem:

$$\begin{aligned}
\text{given} \quad & \{p(a,b|\omega_x,\omega_y)\}_{a,b,x,y} \\
\text{find} \quad & \{\tilde{M}^{\mathrm{A_0B_0}}_{a,b}\}_{a,b} \\
\text{s.t.} \quad & p(a,b|\omega_x,\omega_y) = \mathrm{Tr}[M^{\mathrm{A_0B_0}}_{a,b}(\omega^{\mathrm{A_0}}_{x} \otimes \omega^{\mathrm{B_0}}_{y})] \quad \forall a,b,x,y, \\
& \{M^{\mathrm{A_0B_0}}_{a,b}\}_{a,b} \in \mathscr{S}
\end{aligned} \tag{6.7}$$

where $\mathscr{S}$ denotes the subset of $\mathscr{M}$ which are separable operators, *i.e.*

$$\mathscr{S} = \Big\{\{M^{\mathrm{A_0B_0}}_{a,b}\}_{a,b} | \{M^{\mathrm{A_0B_0}}_{a,b}\}_{a,b} \in \mathscr{M}, \quad M^{\mathrm{A_0B_0}}_{a,b} = \sum_{\lambda} \tau_{a|\lambda} \otimes \chi_{b|\lambda}, \tau_{a|\lambda} \geq 0, \chi_{b|\lambda} \geq 0\Big\} \tag{6.8}$$

This problem is in principle hard to solve, due to the lack of the efficient characterization of the set of separable operators. However one can relax the constraint of separability, and impose instead that each operator $M^{\mathrm{A_0B_0}}_{a,b}$ is positive under partial transpose (PPT). In the feasibility problem above this amounts to replacing the condition $M^{\mathrm{A_0B_0}}_{a,b} = \sum_{\lambda} \tau_{a|\lambda} \otimes \chi_{b|\lambda}, \tau_{a|\lambda} \geq 0, \chi_{b|\lambda} \geq 0$ by $(M^{\mathrm{A_0B_0}}_{a,b})^{T_{\mathrm{A_0}}} \geq 0 \; \forall \; a,b$. With this replacement, the problem becomes a feasibility SDP optimisation problem, which can then be solved efficiently.

Notice however that this relaxation is not able to detect PPT entangled states. A second, more stringent, relaxation of the set of separable operators is the set of the operators having a k-symmetric extension [DPS02]. Imposing that the operators $M^{\mathrm{A_0B_0}}_{a,b}$ have a k symmetric extension amounts to demanding that there exist a $(k+1)$-partite operator $N^{\mathrm{A_0B_0 \ldots B_{k-1}}}_{a,b} \geq 0$ such that $N^{\mathrm{A_0B}_i}_{a,b} = M^{\mathrm{A_0B_0}}_{a,b} \; \forall \; i$. For every fixed k, the above feasibility optimisation problem with this replacement is again an SDP feasibility problem, which now can also detect PPT entangled states [DPS04]. Finally, we note that by increasing the order k of the extension, we obtain stronger SDP tests that converge to the separability test above in the limit of $k \to \infty$.

Finally, it is an important fact that once the sets of quantum inputs used are tomographically complete, then the probabilities $p(a,b|\omega_x,\omega_y)$ allow for an exact reconstruction of the effective POVM elements $M^{\mathrm{A_0B_0}}_{a,b}$, using quantum process tomography. In this special case, *any* available entanglement criterion, not just those that can be checked via SDP, can be used to determine if it is a separable operator or not, leading directly to a conclusion of whether or not the shared state was entangled.

6.2 Measurement-device-independent entanglement estimation

One step beyond certifying the presence of entanglement in a system is to estimate how much entanglement it contains. As discussed in Chapter 2 Section 2.1.2 there are many different entanglement measures, but they are in general not easy to compute even if one knows the full state of the system . In fact the problem of deciding if a given quantum state is entangled is NP-hard, which implies hardness of computing entanglement measures. Quantification of entanglement in a measurement-device-independent scenario was the subject of Ref. [SHR17] where the authors define the best possible pay-off in a semi-quantum games that a state can achieve as an entanglement measure. In what follows we show how to place measurement-device-independent bounds on two well-known entanglement quantifiers, the robustness [VT99] and the negativity [VW02].

6.2.1 MDI lower bound on the robustness of entanglement

A physically well motivated way of quantifying entanglement is through its robustness to noise [VT99], defined as the amount of noise one can add to an entangled state before it becomes separable. As already shown in Section 2.1.2, the generalized robustness r_g of a state ρ is given by

$$\begin{aligned} r_S(\rho^{\mathrm{AB}}) = \min_{r,\sigma^{\mathrm{AB}}} \quad & r \\ \text{s.t.} \quad & \frac{\rho^{\mathrm{AB}} + r\sigma^{\mathrm{AB}}}{1+r} \in SEP, \\ & \sigma^{\mathrm{AB}} \in S \end{aligned} \tag{6.9}$$

where S is a subset of quantum states, which defines the type of robustness, and SEP denotes the set of separable states. Typical choices for S include the set of all quantum states (generalized robustness), the set of separable states (classical robustness) or the maximally mixed state (random robustness).

In a similar way we define the robustness of MDI-nonlocality $\tilde{r}_S^{MDI}$ as the minimum amount of noise that has to be added to the set of probability distributions $\{p(a,b|\omega_x,\omega_y)\}$ before it can be reproduced by a separable state, where the noise comes from the set S. Formally, the MDI-nonlocality robustness is the solution of the following optimization problem

$$\tilde{r}_S^{MDI}[p(a,b|\omega_x,\omega_y)] = \min_{\{M_{a,b}^{\mathrm{A_0B_0}}\}_{a,b},\{N_{a,b}^{\mathrm{A_0B_0}}\}_{a,b}} \quad r \tag{6.10}$$

$$\begin{aligned}\text{s.t.}\quad & \frac{p(a,b|\omega_x,\omega_y)+r\pi(a,b|\omega_x,\omega_y)}{1+r} = \mathrm{Tr}[M_{a,b}^{\mathrm{A_0B_0}}(\omega_x^{\mathrm{A_0}}\otimes\omega_y^{\mathrm{B_0}})],\\ & \pi(a,b|\omega_x,\omega_y) = \mathrm{Tr}[N_{a,b}^{\mathrm{A_0B_0}}(\omega_x^{\mathrm{A_0}}\otimes\omega_y^{\mathrm{B_0}})] \quad \forall a,b,x,y,\\ & \{M_{a,b}^{\mathrm{A_0B_0}}\}_{a,b}\in\mathscr{S}, \qquad \{N_{a,b}^{\mathrm{A_0B_0}}\}_{a,b}\in\mathscr{M}_S.\end{aligned}$$

where $\mathscr{M}_S$ is the set of effective POVMs associated to the noise S. For example, for the generalized robustness, when the set S corresponds to all quantum states, then $\mathscr{M}_S=\mathscr{M}$. Similarly, for the robustness, when the set S corresponds to all separable states, then $\mathscr{M}_S=\mathscr{S}$. Finally, for the random robustness, when $S=\{\mathbb{1}^{\mathrm{AB}}/d_{\mathrm{A}}d_{\mathrm{B}}\}$, then $\mathscr{M}_S=\left\{\{\tilde{M}_{a,b}^{\mathrm{A_0B_0}}\}_{a,b}|\{M_{a,b}^{\mathrm{A_0B_0}}\}_{a,b}\in M, M_{a,b}^{\mathrm{A_0B_0}}=M_a^{\mathrm{A_0}}\otimes M_b^{\mathrm{B_0}}\right\}$.

We now show that $\tilde{r}_S^{MDI}$ is a lower bound to the robustness of entanglement r_S of the underlining state being measured. To see this consider that the robustness of the state ρ^{AB} is given by r_S^*. This means that there exist a state $\sigma^{*\mathrm{AB}}\in S$ for which the state $(\rho+r_S^*\sigma^*)/(1+r_S^*)$ is separable. Thus for any POVMs $\{M_a^{\mathrm{A_0A}}\}_a$ and $\{M_b^{\mathrm{B_0B}}\}_b$ satisfying (6.1),

$$M_{a,b}^{\mathrm{A_0B_0}} = \mathrm{Tr}_{\mathrm{AB}}\left[\left(M_a^{\mathrm{A_0A}}\otimes M_b^{\mathrm{BB_0}}\right)\left(\mathbb{1}^{\mathrm{A_0}}\otimes\frac{\rho^{\mathrm{AB}}+r_S^*\sigma^{*\mathrm{AB}}}{1+r_S^*}\otimes\mathbb{1}^{\mathrm{B_0}}\right)\right], \tag{6.11}$$

and

$$N_{a,b}^{\mathrm{A_0B_0}} = \mathrm{Tr}_{\mathrm{AB}}\left[\left(M_a^{\mathrm{A_0A}}\otimes M_b^{\mathrm{BB_0}}\right)\left(\mathbb{1}^{\mathrm{A_0}}\otimes\sigma^{*\mathrm{AB}}\otimes\mathbb{1}^{\mathrm{B_0}}\right)\right], \tag{6.12}$$

are feasible for the problem (6.10) (i.e. satisfy all the constraints) and achieve the value $r=r_S^*$, as can be verified by direct substitution. Since $\{M_{a,b}^{\mathrm{A_0B_0}}\}_{a,b}$ and $\{N_{a,b}^{\mathrm{A_0B_0}}\}_{a,b}$ given by Eqs. (6.11) and (6.12) do not necessarily provide an optimal solution to the problem (6.10), then

$$\tilde{r}_S^{MDI}[p(a,b|\omega_x,\omega_y)] \leq r_S^*(\rho^{\mathrm{AB}}). \tag{6.13}$$

This bound can be easily interpreted. If the measured state is separable, *i.e.* $r_S^*(\rho^{\mathrm{AB}})=0$, then the probability distribution obtained by measuring it trivially has a separable realisation, so $\tilde{r}_S^{MDI}[p(a,b|\omega_x,\omega_y)]=0$. On the other hand, if Alice and Bob detect that $\tilde{r}_S^{MDI}[p(a,b|\omega_x,\omega_y)]>0$, then they immediately conclude that the underlining state is entangled, and moreover can place a lower bound on the amount of entanglement, as measured by the robustness (with respect to S), that is necessary to explain the data.

6.2.2 MDI lower bound on the negativity

Another widely used entanglement measure of entanglement is the negativity [VW02]. Analogously to the device-independent estimation of negativity [Mor+13] it is possible to put a lower bound on the negativity in a measurement-device-independent way. As discussed in Section 2.1.2 the negativity $\mathcal{N}$ of some state ρ^{AB} is defined as the sum of the absolute values of the non-positive eigenvalues of the partially transposed state $\rho^{T_{\mathrm{A}}}$. It has been shown in Ref. [VW02] that it admits the following representation

$$\begin{aligned}\mathcal{N}(\rho^{\mathrm{AB}}) = \min_{\rho_+,\rho_-} \quad & \mathrm{Tr}[\rho_-], \\ \text{s.t.} \quad & \rho^{\mathrm{AB}} = \rho_+ - \rho_-, \\ & \rho_\pm^{T_{\mathrm{A}}} \geq 0.\end{aligned} \tag{6.14}$$

Having in mind the decomposition $\rho^{\mathrm{AB}} = \rho_+ - \rho_-$ it is possible to write the observed probabilities from the quantum inputs scenario in the following way

$$\begin{aligned} p(a,b|\omega_x,\omega_y) &= \mathrm{Tr}\left[\left(M_a^{\mathrm{A_0A}} \otimes M_b^{\mathrm{BB_0}}\right)\left(\omega_x^{\mathrm{A_0}} \otimes \rho^{\mathrm{AB}} \otimes \omega_y^{\mathrm{B_0}}\right)\right] \\ &= q_+(a,b|\omega_x,\omega_y) - q_-(a,b|\omega_x,\omega_y), \end{aligned}$$

where

$$\begin{aligned} q_+(a,b|\omega_x,\omega_y) &= \mathrm{Tr}\left[\left(M_a^{\mathrm{A_0A}} \otimes M_b^{\mathrm{BB_0}}\right)\left(\omega_x^{\mathrm{A_0}} \otimes \rho_+ \otimes \omega_y^{\mathrm{B_0}}\right)\right], \\ q_-(a,b|\omega_x,\omega_y) &= \mathrm{Tr}\left[\left(M_a^{\mathrm{A_0A}} \otimes M_b^{\mathrm{BB_0}}\right)\left(\omega_x^{\mathrm{A_0}} \otimes \rho_- \otimes \omega_y^{\mathrm{B_0}}\right)\right]. \end{aligned}$$

According to Eq. (6.14) the negativity can be obtained by minimizing $\mathrm{tr}[\rho_-]$, which can be written as

$$\begin{aligned} &\sum_{a,b} q_-(a,b|\omega_x,\omega_y) \\ &\quad = \mathrm{Tr}\left[\left(\sum_a M_a^{\mathrm{A_0A}} \otimes \sum_b M_b^{\mathrm{BB_0}}\right)\left(\omega_x^{\mathrm{A_0}} \otimes \rho_- \otimes \omega_y^{\mathrm{B_0}}\right)\right] \\ &\quad = \mathrm{Tr}[\rho_-]. \end{aligned} \tag{6.15}$$

In order to estimate the negativity by an SDP optimization it is necessary to understand the form an effective POVM $M_{a,b}$ corresponding to a PPT state. We recall that for an arbitrary state an effective POVM must be positive and satisfy no-signalling principle, as encoded in Eq. (6.5), and for a separable state it also has to be a separable operator, as encoded in Eq. (6.8). An effective POVM corresponding to a PPT state, besides satisfying the no-signalling constraints, must also be a PPT operator. To see this consider partial transpose of an effective POVM

$$\begin{aligned} \left(M_{a,b}^{\mathrm{A_0B_0}}\right)^{T_{\mathrm{A_0}}} &= \mathrm{Tr}_{\mathrm{AB}}\left[\left(\left(M_a^{\mathrm{A_0A}}\right)^{T_{\mathrm{A_0}}} \otimes M_b^{\mathrm{BB_0}}\right)\left(\mathbb{1}^{\mathrm{A_0}} \otimes \rho^{\mathrm{AB}} \otimes \mathbb{1}^{\mathrm{B_0}}\right)\right], \\ &= \mathrm{Tr}_{\mathrm{AB}}\left[\left(\left(M_a^{\mathrm{A_0A}}\right)^{T} \otimes M_b^{\mathrm{BB_0}}\right)\left(\mathbb{1}^{\mathrm{A_0}} \otimes \left(\rho^{\mathrm{AB}}\right)^{T_{\mathrm{A}}} \otimes \mathbb{1}^{\mathrm{B_0}}\right)\right]. \end{aligned}$$

The second equality follows from the fact that $\mathrm{tr}[A^T B] = \mathrm{tr}[AB^T]$. Since the full transpose is a CPTP map, $\left(M_a^{\mathrm{A_0A}}\right)^T$ is a positive operator and thus $\left(M_{a,b}^{\mathrm{A_0B_0}}\right)^{T_{\mathrm{A_0}}}$ is positive if the state ρ^{AB} is PPT, which is exactly the claim we wanted to prove. We will denote by $\mathscr{P}$ the set of effective POVMs that are also PPT, i.e.

$$\mathscr{P} = \left\{ \{M_{a,b}^{\mathrm{A_0B_0}}\}_{a,b} | \{M_{a,b}^{\mathrm{A_0B_0}}\}_{a,b} \in \mathscr{M}, \left(M_{a,b}^{\mathrm{A_0B_0}}\right)^{T_{\mathrm{A_0}}} \geq 0 \right\} \tag{6.16}$$

Now we have all the ingredients for the formulation of the SDP whose solution lower bounds the negativity of a state compatible with some observed probability distribution $p(a,b|\omega_x,\omega_y)$ in the quantum input scenario:

$$\begin{aligned} N^{MDI}[p(a,b|\omega_x,\omega_y)] = & \min_{\{M_{\pm,a,b}^{\mathrm{A_0B_0}}\}_{a,b}} \sum_{a,b} q_-(a,b|\omega_x,\omega_y), \\ \text{s.t.} \quad & p(a,b|\omega_x,\omega_y) = q_+(a,b|\omega_x,\omega_y) - q_-(a,b|\omega_x,\omega_y), \\ & q_\pm(a,b|\omega_x^{\mathrm{A_0}},\omega_y^{\mathrm{B_0}}) = \mathrm{Tr}\left[M_{\pm,a,b}^{\mathrm{A_0B_0}}(\omega_x \otimes \omega_y)\right], \quad \forall a,b \\ & \{M_{\pm,a,b}^{\mathrm{A_0B_0}}\}_{a,b} \in \mathscr{P} \end{aligned} \tag{6.17}$$

6.3 Multipartite case

In this section we generalize the previous entanglement detection and quantification techniques to the multipartite scenario. In Buscemi's paper [Bus12] there is an outline of the proof that all multipartite entangled states exhibit some kind of nonlocality when queried with quantum inputs. Moreover, the approach via entanglement witnesses is also explained in Ref. [BRLG13], but as in the bipartite case the witness is tailored for a specific state. Here, as before, we are interested in the detection of multipartite entanglement without a priori knowledge of the system under study.

In the bipartite case we saw that the problem reduces to finding a separable effective POVM that returns the observed data when applied to the chosen set of inputs. This generalizes to the multipartite case as follows: given a certain type of separability, we want to find the properties of the effective POVM which by acting on the given set of quantum inputs returns the observed probability distribution. As expected, we will show that the effective POVM should have the same type of separability properties as the underlying state. For the sake of simplicity we will consider the tripartite scenario, with the generalization to more parties being straightforward.

The scenario involves three parties, Alice, Bob and Charlie, each of whom can input quantum systems in the states ω_x, ω_y and ω_z respectively in their measuring devices, that subsequently provide classical outputs a, b and c. The experiment is characterized by the set of joint probabilities of the form

$$p(a,b,c|\omega_x,\omega_y,\omega_z) = \mathrm{Tr}\left[\left(M_a^{\mathrm{A_0A}} \otimes M_b^{\mathrm{B_0B}} \otimes M_c^{\mathrm{C_0C}}\right)\left(\rho^{\mathrm{ABC}} \otimes \omega_x^{\mathrm{A_0}} \otimes \omega_y^{\mathrm{B_0}} \otimes \omega_z^{\mathrm{C_0}}\right)\right], \tag{6.18}$$

where $M_a^{\mathrm{A_0A}}$ is a POVM Alice applies to the input ψ_x and her share of the state ρ^{ABC}, and analogous for $M_b^{\mathrm{B_0B}}$ and $M_c^{\mathrm{C_0C}}$. In the same way as in the bipartite scenario it is useful to define an effective POVM

$$M_{a,b,c}^{\mathrm{A_0B_0C_0}} = \mathrm{Tr}_{\mathrm{ABC}}\left[\left(M_a^{\mathrm{A_0A}} \otimes M_b^{\mathrm{B_0B}} \otimes M_c^{\mathrm{C_0C}}\right)\left(\rho^{\mathrm{ABC}} \otimes \mathbb{1}^{\mathrm{A_0B_0C_0}}\right)\right] \tag{6.19}$$

which allows one to write

$$p(a,b,c|\omega_x,\omega_y,\omega_z) = \mathrm{Tr}\left[M_{a,b,c}^{\mathrm{A_0B_0C_0}}(\omega_x^{\mathrm{A_0}} \otimes \omega_y^{\mathrm{B_0}} \otimes \omega_z^{\mathrm{C_0}})\right]. \tag{6.20}$$

As in the bipartite case, the effective POVM elements satisfy a number of constraints by construction, which play the role of no-signalling conditions. For example

$$\sum_a M_{a,b,c}^{\mathrm{A_0B_0C_0}} = \mathbb{1}^{\mathrm{A_0}} \otimes M_{b,c}^{\mathrm{B_0C_0}}, \tag{6.21}$$

with $M_{b,c}^{\mathrm{B_0C_0}}$ another effective POVM for Bob and Charlie. We will denote the set of effective POVMs which satisfy all such conditions in the tripartite case by $\mathscr{M}^{\mathrm{ABC}}$.

In what follows we show that the entanglement properties of the effective POVM elements (6.19) are the same as entanglement properties of the shared state ρ^{ABC} .

Fully separable states can be written in the form $\rho^{\mathrm{ABC}} = \sum_\lambda p_\lambda \rho_\lambda^{\mathrm{A}} \otimes \rho_\lambda^{\mathrm{B}} \otimes \rho_\lambda^{\mathrm{C}}$ and if Alice, Bob and Charlie share such a state the corresponding effective POVM elements (6.19) will also be fully separable operators

$$M_{a,b,c}^{\mathrm{A_0B_0C_0}} = \sum_\lambda p_\lambda M_{a|\lambda}^{\mathrm{A_0}} \otimes M_{b|\lambda}^{\mathrm{B_0}} \otimes M_{c|\lambda}^{\mathrm{C_0}} \tag{6.22}$$

where $M_{a|\lambda}^{\mathrm{A_0}} = \mathrm{Tr}_{\mathrm{A}}\left[M_a^{\mathrm{A_0A}}\left(\mathbb{1}^{\mathrm{A_0}} \otimes \rho_\lambda^{\mathrm{A}}\right)\right]$ is an effective POVM, and analogously for $M_{b|\lambda}^{\mathrm{B_0}}$ and $M_{c|\lambda}^{\mathrm{C_0}}$. Analogously to the bipartite case, we define a subset $\mathscr{S}^{\mathrm{A|B|C}}$ of all effective tripartite POVMs $\mathscr{M}^{\mathrm{ABC}}$, which are also fully separable,

$$\begin{aligned}\mathscr{S}^{\mathrm{A|B|C}} = \Big\{\{M_{a,b,c}^{\mathrm{A_0B_0C_0}}\}_{a,b,c} | \{M_{a,b,c}^{\mathrm{A_0B_0C_0}}\}_{a,b,c} \in \mathscr{M}^{\mathrm{ABC}}, M_{a,b,c}^{\mathrm{A_0B_0C_0}} =& \\ = \sum_\lambda \tau_{a|\lambda} \otimes \chi_{b|\lambda} \otimes \omega_{c|\lambda}, \tau_{a|\lambda} \geq 0, \chi_{b|\lambda} \geq 0, \omega_{c|\lambda} \geq 0\Big\}.&\end{aligned}$$

With this in place, full separability of the shared state can thus be cast by the following feasibility problem:

$$\begin{aligned}
\text{given} \quad & \{p(a,b,c|\omega_x,\omega_y,\omega_z)\}_{a,b,c,x,y,z}, \\
\text{find} \quad & \{M_{a,b,c}^{\mathrm{A_0B_0C_0}}\}_{a,b,c} \\
\text{s.t.} \quad & p(a,b,c|\omega_x,\omega_y,\omega_z) = \mathrm{Tr}\big[M_{a,b,c}^{\mathrm{A_0B_0C_0}}(\omega_x^{\mathrm{A_0}}\otimes\omega_y^{\mathrm{B_0}}\otimes\omega_z^{\mathrm{C_0}})\big] \\
& \qquad\qquad \forall a,b,c,x,y,z \\
& \{M_{a,b,c}^{\mathrm{A_0B_0C_0}}\}_{a,b,c} \in \mathscr{S}^{\mathrm{A|B|C}}
\end{aligned} \tag{6.23}$$

In the similar way as in the bipartite scenario, it is necessary to choose an appropriate relaxation of the set of fully separable tripartite operators in order to turn this feasibility problem into an SDP. The set of operators which are PPT across all biparititons is one choice. A second option is to use the multipartite generalisation of the k-shareability hierarchy of SDPs [Doh14].

Recall that tripartite states have a richer entanglement structure than bipartite states, such that even if the problem (6.23) confirms that there is some entanglement in the system, a full entanglement characterization is not yet complete. It can happen, for example, that the entanglement is shared only between two parties. States which have such entanglement structure are called separable across a certain bipartition. For example the state $\rho^{\mathrm{ABC}} = \sum_\lambda p_\lambda \rho_\lambda^{\mathrm{AB}} \otimes \rho_\lambda^{\mathrm{C}}$ is separable with respect to the bipartition AB$|$C. A state is biseparable if it can be written as a convex combination of the states that are separable with respect to different bipartitions:

$$\rho^{\mathrm{ABC}} = \sum_\lambda p_\lambda^{\mathrm{A|BC}} \rho_\lambda^{\mathrm{A}} \otimes \rho_\lambda^{\mathrm{BC}} + \sum_\mu p_\mu^{\mathrm{B|AC}} \rho_\mu^{\mathrm{B}} \otimes \rho_\mu^{\mathrm{AC}} + \sum_\nu p_\nu^{\mathrm{C|AB}} \rho_\nu^{\mathrm{AB}} \otimes \rho_\nu^{\mathrm{C}}. \tag{6.24}$$

The strongest form of entanglement that can be present in a tripartite system is genuine multipartite entanglement (GME). A state ρ^{ABC} is genuinely multipartite entangled if it is not biseparable.

Let us assume that the state shared between Alice, Bob and Charlie is biseparable (6.24). In that case the effective POVM reads

$$M_{a,b,c}^{\mathrm{A_0B_0C_0}} = \sum_\lambda p_\lambda^{\mathrm{A|BC}} M_{a|\lambda}^{\mathrm{A_0}} \otimes M_{b,c|\lambda}^{\mathrm{B_0C_0}} + \sum_\mu p_\mu^{\mathrm{B|AC}} M_{b|\mu}^{\mathrm{B_0}} \otimes M_{a,c|\mu}^{\mathrm{A_0C_0}} + \sum_\nu p_\nu^{\mathrm{AB|C}} M_{a,b|\nu}^{\mathrm{A_0B_0}} \otimes M_{c|\nu}^{\mathrm{C_0}}, \tag{6.25}$$

where

$$\begin{aligned}
M_{a|\lambda}^{\mathrm{A_0}} &= \mathrm{Tr}\left[M_a^{\mathrm{A_0A}}\left(\omega_x^{\mathrm{A_0}}\otimes\rho_\lambda^{\mathrm{A}}\right)\right], \\
M_{b,c|\lambda}^{\mathrm{A_0}} &= \mathrm{Tr}\left[\left(M_b^{\mathrm{B_0B}}\otimes M_c^{\mathrm{CC_0}}\right)\left(\omega_y^{\mathrm{B_0}}\otimes\rho_\lambda^{\mathrm{BC}}\otimes\omega_z^{\mathrm{C_0}}\right)\right]
\end{aligned}$$

and analogously for all other operators. Thus, the fact that the state ρ^{ABC} is biseparable implies that the operators (6.25) are also biseparable.

With this structure in mind it is possible to construct a feasibility problem to test whether an observed probability distribution in the quantum input scenario can be obtained with a biseparable state:

$$\begin{aligned}
\text{given}\quad & \{p(a,b,c|\omega_x,\omega_y,\omega_z)\}_{a,b,c,x,y,z}, \\
\text{find}\quad & \{M_{a|b,c}^{\mathrm{A_0B_0C_0}}, M_{b|a,c}^{\mathrm{A_0B_0C_0}}, M_{c|a,b}^{\mathrm{A_0B_0C_0}}\}_{a,b,c} \\
\text{s.t.}\quad & p(a,b,c|\omega_x,\omega_y,\omega_z) = \mathrm{Tr}\big[M_{a,b,c}^{\mathrm{A_0B_0C_0}}(\omega_x^{\mathrm{A_0}}\otimes\omega_y^{\mathrm{B_0}}\otimes\omega_z^{\mathrm{C_0}})\big] \\
& \qquad \forall a,b,c,x,y,z \\
& M_{a,b,c}^{\mathrm{A_0B_0C_0}} = M_{a|b,c}^{\mathrm{A_0B_0C_0}} + M_{b|a,c}^{\mathrm{A_0B_0C_0}} + M_{c|a,b}^{\mathrm{A_0B_0C_0}} \quad \forall a,b,c \\
& \{M_{a|b,c}^{\mathrm{A_0B_0C_0}}\}_{a,b,c} \in \mathscr{S}^{\mathrm{A|B,C}}, \quad \{M_{b|a,c}^{\mathrm{A_0B_0C_0}}\}_{a,b,c} \in \mathscr{S}^{\mathrm{B|A,C}}, \\
& \{M_{c|a,b}^{\mathrm{A_0B_0C_0}}\}_{a,b,c} \in \mathscr{S}^{\mathrm{C|A,B}}.
\end{aligned} \tag{6.26}$$

where $\mathscr{S}^{\mathrm{A|B,C}}$ denotes the subset of effective tripartite POVMs $\mathscr{M}^{\mathrm{ABC}}$ that are also separable across the bipartition $\mathrm{A|B,C}$ and analogously for $\mathscr{S}^{\mathrm{B|A,C}}$ and $\mathscr{S}^{\mathrm{C|A,B}}$. Once more, by replacing the sets $\mathscr{S}$ by the set of PPT operators or operators having k-symmetric extension the above problem becomes an instance of a SDP.

Quantification of multipartite entanglement can be performed in a similar manner as in the bipartite scenario. Namely, one can lower bound the robustness of genuine multipartite entanglement, or simply robustness of multipartite entanglement, by defining MDI multipartite nonlocality robustness analogously to (6.10).

6.4 Randomness from quantum inputs

Nonlocal correlations, as proven by Bell's theorem, cannot be explained by any classical, deterministic model or a convex combinations of such models. Consequently, a violation of a Bell inequality can be used to certify that the data generated is intrinsically random. As explained in Section 2.6 this reasoning led to the development of the protocols for so-called device-independent randomness certification [AM16]. In these protocols the amount of (global) randomness stemming from some Bell experiment is characterized by the guessing probability $G_{x,y}$ with which an external eavesdropper can guess a pair of outcomes observed by Alice and Bob when they make measurements x and y. A lower bound on the guessing probability is

$$G_{x^*,y^*} = \max_{a,b} p(a,b|x^*,y^*). \tag{6.27}$$

and this is the best that an external observer uncorrelated with Alice and Bob can guess. However, an eavesdropper, usually named Eve, can have side-information – a system that is correlated (or even entangled) with the state of Alice and Bob. In principle she could have even provided all the measuring devices, and can possibly achieve much better guessing probability than the lower bound (6.27). Thus the aim of a device-independent randomness estimation protocol is to quantify the randomness of Alice's (and/or Bob's) measurement outcomes by optimizing over all possible eavesdropping strategies of Eve compatible with the obtained Bell inequality violation. The scenario assumes that by sharing a tripartite state, and performing some measurement on her share, Eve steers the state of Alice and Bob. Her strategy is to perform a measurement such that her outcome, denoted by e, will give her the highest probability to guess the pair of outcomes for one particular choice of measurements for Alice and Bob.

In such a scenario calculating Eve's guessing probability, if the obtained value of a Bell expression $\sum_{a,b,x,y} b_{a,b,x,y} p(a,b|x,y)$ is equal to $\mathscr{I}$ can be cast as the following optimisation problem

$$\begin{aligned} G_{x^*,y^*} = & \max_{\{p(a,b,e|x,y)\}_{a,b,e,x,y}} \sum_e p(a,b,e=(a,b)|x^*,y^*), \\ & \text{s.t} \sum_{a,b,e,x,y} b_{a,b,x,y} p(a,b,e|x,y) = \mathscr{I}; \\ & \{p(a,b,e|x,y,z)\}_{a,b,e,x,y} \in \mathscr{Q}. \end{aligned} \tag{6.28}$$

where $\mathscr{Q}$ denotes the set of quantum behaviours, i.e. the set of all $\{p(a,b,e|x,y)\}_{a,b,e,x,y}$ that can arise by performing local measurements on a tripartite quantum state. This program gives the highest probability with which Eve's outcome e is the same as Alice's and Bob's outcomes, a and b, for some specific pair of inputs x^* and y^*, with the constraints that the overall probabilities must be compatible with quantum mechanics and the observed violation of a Bell inequality. In general this problem cannot be solved exactly, due to the set $\mathscr{Q}$ having no known simple characterisation (in particular since it implicitly contains all behaviours compatible with any quantum state and measurements in a Hilbert space of any dimension). However, by using the Navascues-Pironio-Acin (NPA) hierarchy of SDP relaxations of the quantum set of behaviours [NPA07], computable upper bounds can be placed on the guessing probability.

One generalization of this protocol to the quantum-input scenario under the name measurement-device-independent randomness certification has been introduced in Ref. [CB15]. Analogously to the ability to detect entanglement of all entangled states, even those that do not violate any Bell inequality, the authors of Ref. [CB15] prove that it is possible to extract randomness from local entangled states in a measurement-device-independent way. They use the analogue of the program (6.28) with the constraint that the probabilities $p(a,b|\omega_x,\omega_y)$ violate the inequality corresponding to a specific MDIEW. As already noted in the previous text, a MDIEW is usually constructed with respect to a specific entangled state. It can nevertheless be used to check if some other entangled state in principle can be useful for randomness extraction. However, as the source providing Alice's and Bob's shared state is uncharacterized it may not be clear which witness should be used, and therefore it is desirable to have a method to certify randomness that does not rely on a specific MDIEW. Another way to certify randomness in the quantum input scenario is the subject of Ref. [CZM15]. In this approach the source has to prepare a tomographically complete set of inputs which are used to perform quantum process tomography of the measurement device. Randomness is generated by measuring one of the prepared quantum inputs by the characterized POVM. A method do quantify the amount of randomness is presented for two-outcome POVMs. This approach was used to experimentally generate randomness in a measurement-device-independent manner [Nie+16].

In the rest of this section we show the way to quantify the amount of randomness resulting from an experiment with quantum inputs without assuming the underlying state. This can be seen as the generalisation of the approach of Refs. [NSPS13, BSS14] from the standard Bell scenario to the quantum inputs scenario. The protocol works for measurements with arbitrary number of outputs and the set of quantum inputs does not have to be tomographically complete, which makes it more general than [CZM15].

Before presenting the more general approach to randomness estimation in the quantum inputs scenario, let us consider in more detail the essential novelty of this scenario, which is the fact that before guessing the measurement outcome Eve has to guess the input state. Due to this it is not only possible to extract randomness from local entangled states as observed in Ref. [CB15], but also from a single black-box, i.e. without the use of entanglement.

This leads us to the change of scenario: now we have only one party, Alice, who has a characterized device which prepares quantum input states ω_x. Alice measures these states using an uncharacterized black box, modelled by POVM $\{M_a\}_a$ and obtains some outcomes a. By repeating the process she can calculate the set of probabilities $p(a|\omega_x)$, to get an outcome a when the quantum input is ω_x. The question is how random Alice's outputs are for Eve. In some cases Alice can be sure that her outcomes are genuinely random. If the set of quantum inputs is tomographicaly complete Alice can perform process tomography and exactly learn which POVM her black-box is applying. In the special case when the obtained POVM is extremal Eve cannot be correlated with Alice's experiment because extremal POVMs cannot be decomposed as a convex combination of other POVMs. Therefore Eve's guessing probability is obtained simply from (6.27) (restricted to a single party Alice, instead of Alice and Bob). An extremal d-dimensional POVMs cannot have more than d^2 outcomes [DPP05], which means that when preparing qubit quantum inputs Alice at best can get 2 bits of randomness. One example is the case when Alice prepares the following informationally complete set of quantum inputs $\{\frac{\mathbb{1}}{2}, |0\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle+i|1\rangle}{\sqrt{2}}\}$ and observes the probability distribution which corresponds to measuring these inputs with an extremal four-outcome tetrahedral POVM. The probabilities to get any of the four outcomes when measuring the input which is in the maximally mixed state $\frac{\mathbb{1}}{2}$ is equal to 0.25, which corresponds to 2 bits of randomness.

In the general case, when the set of quantum inputs is not tomographically complete, or the applied POVM is not extremal it is still possible to construct an SDP-based estimation of randomness analogous to (6.28). Since the measuring device is uncharacterized it has to be assumed that it was possibly prepared by Eve. In that case Eve can be quantumly correlated with the box. That is, she can prepare an ancillary entangled pair of particles ρ^{AE}, and place half inside the box, while keeping the other half. In each round Alice's box then performs a joint measurement $M_a^{\mathrm{A_0 A}}$, where a corresponds to Alice's outcome, and Eve performs a measurement N_e^{E}, with outcome e. Thus, the probability for Alice to get outcome a and Eve to get e, when the quantum input is ${\omega_x}^{\mathrm{A_0}}$ is

$$\begin{aligned} p(a,e|\omega_x) &= \mathrm{Tr}\left[\left(M_a^{\mathrm{A_0A}} \otimes N_e^{\mathrm{E}}\right)\left(\omega_x^{\mathrm{A_0}} \otimes \rho^{\mathrm{AE}}\right)\right] \\ &= \mathrm{tr}[M_{a,e}^{\mathrm{A_0}} \omega_x^{\mathrm{A_0}}] \end{aligned} \tag{6.29}$$

where $M_{a,e}$ is an effective POVM which satisfies the relation

$$M_{a,e}^{\mathrm{A_0}} = \mathrm{Tr_{AE}}\left[\left(M_a^{\mathrm{A_0A}} \otimes N_e^{\mathrm{E}}\right)\left(\mathbb{1}^{\mathrm{A_0}} \otimes \rho^{\mathrm{AE}}\right)\right]. \tag{6.30}$$

From this relation, it follows that the effective POVM satisfies the relation

$$\sum_a M_{a,e}^{\mathrm{A_0}} = p(e)\mathbb{1}^{\mathrm{A_0}}, \tag{6.31}$$

where $p(e) \geq 0$. As in the above, this can be seen as the no-signalling constraint from Alice to Eve.

With the above in place, the optimisation problem which bounds the guessing probability of Eve is

$$\begin{aligned} G_{x^*} = \max_{\{M_{a,e}^{\mathrm{A_0}}\}_{a,e}} \quad & \mathrm{tr}\sum_e M_{a=e,e}^{\mathrm{A_0}} \omega_{x^*}^{\mathrm{A_0}}, \\ \text{s.t} \quad & \mathrm{tr}\sum_e M_{a,e}^{\mathrm{A_0}} \omega_x^{\mathrm{A_0}} = p(a|\omega_x), \quad \forall x, a; \\ & \sum_a M_{a,e}^{\mathrm{A_0}} = p(e)\mathbb{1}^{\mathrm{A_0}}, \quad \sum_e p(e) = 1, \quad \forall e. \end{aligned} \tag{6.32}$$

The objective function maximizes the probability for Eve to guess the outcome a when Alice measures the quantum input $\omega_x^{\mathrm{A_0}}$, by optimizing over all possible effective POVMs $M_{a,e}^{\mathrm{A_0}}$. The first constraint ensures that that effective POVMs are in accordance with the observed probability distribution, while the second imposes no-signalling and completeness of the measurement. For any probability distribution obtained by measuring some set of quantum inputs, the above optimisation problem, which is an SDP, gives the guessing probability, and thus the randomness of the outcomes.

A similar analysis can be applied in the bipartite case. As mentioned above, in the standard Bell scenario one does not need to consider a specific Bell inequality in order for randomness estimation, but rather can use the full nonlocal behaviour (set of correlations) obtained in a Bell experiment [NSPS13, BSS14]. In what follows we generalize this method, providing an alternative way to quantify randomness in a measurement-device-independent manner. Specifically we show that it is possible to certify randomness even when Alice and Bob share a separable state.

In the scenario with quantum inputs Eve again distributed a state to Alice and Bob with which she is entangled. By performing a local POVM N_e on her share, and conditioned on the outcome e, she prepares an subnormalized state ρ_e^{AB}, whose norm is equal to the probability for Eve to obtain the outcome $\mathrm{Tr}\rho_e^{\mathrm{AB}} = p(e)$. The full joint probability is given by

$$\begin{aligned} p(a,b,e|\omega_x,\omega_y) &= \mathrm{Tr}\left[\left(M_a^{\mathrm{A_0A}} \otimes M_b^{\mathrm{BB_0}}\right)\left(\omega_x^{\mathrm{A_0}} \otimes \rho_e^{\mathrm{AB}} \otimes \omega_y^{\mathrm{B_0}}\right)\right] \\ &= \mathrm{Tr}\left[M_{a,b,e}^{\mathrm{A_0B_0}}\left(\omega_x^{\mathrm{A_0}} \otimes \omega_y^{\mathrm{B_0}}\right)\right] \end{aligned} \tag{6.33}$$

where $M_{a,b,e}$ is an effective POVM defined by

$$M_{a,b,e}^{\mathrm{A_0B_0}} = \mathrm{Tr_{AB}}\left[\left(M_a^{\mathrm{A_0A}} \otimes M_b^{\mathrm{BB_0}}\right)\left(\mathbb{1}^{\mathrm{A_0}} \otimes \rho_e^{\mathrm{AB}} \otimes \mathbb{1}^{\mathrm{B_0}}\right)\right]. \tag{6.34}$$

These effective POVMs, apart from satisfying the completeness relation $\sum_{a,b,e} M_{a,b,e}^{\mathrm{A_0B_0}} = \mathbb{1}^{\mathrm{A_0B_0}}$ also satisfy the no-signalling constraints

$$\begin{aligned} \sum_a M_{a,b,e}^{\mathrm{A_0B_0}} &= \mathbb{1}^{\mathrm{A_0}} \otimes M_{b,e}^{\mathrm{B_0}}, \\ \sum_b M_{a,b,e}^{\mathrm{A_0B_0}} &= M_{a,e}^{\mathrm{A_0}} \otimes \mathbb{1}^{\mathrm{B_0}}, \end{aligned} \tag{6.35}$$

where $\{M_{b,e}^{\mathrm{B_0}}\}_b$ and $\{M_{a,e}^{\mathrm{A_0}}\}_b$ are subnormalized POVMs (for Bob and Alice respectively), for all values of e, with the same normalisation for each e, i.e. $\sum_b M_{b,e}^{\mathrm{B_0}} = p(e)\mathbb{1}^{\mathrm{B_0}}$ and $\sum_a M_{a,e}^{\mathrm{A_0}} = p(e)\mathbb{1}^{\mathrm{A_0}}$.

Like in the standard Bell scenario Eve's optimal strategy is to perform a measurement such that the outcome e will be equal to the pair (a,b) with a probability as high as possible, for some specific pair of quantum inputs $\omega_{x^*}^{\mathrm{A_0}}$ and $\omega_{y^*}^{\mathrm{B_0}}$. Eve's optimal guessing probability is then the solution of the following SDP

$$
\begin{aligned}
G^{MDI}_{x^*,y^*} = \max_{\{M_{a,b,e}\}^{\mathrm{A_0B_0}}_{a,b,e}} \quad & \operatorname{tr}\sum_e M^{\mathrm{A_0B_0}}_{a,b,e=(a,b)}\left(\omega^{\mathrm{A_0}}_{x^*}\otimes\omega^{\mathrm{B_0}}_{y^*}\right), \\
\text{s.t} \quad & \operatorname{tr}\sum_e M^{\mathrm{A_0B_0}}_{a,b,e}\left(\omega^{\mathrm{A_0}}_{x}\otimes\omega^{\mathrm{B_0}}_{y}\right) = p(a,b|\omega_x,\omega_y), \forall x,y,a,b, \\
& M^{\mathrm{A_0B_0}}_{a,b,e} \geq 0 \qquad \forall a,b,e, \\
& \sum_a M^{\mathrm{A_0B_0}}_{a,b,e} = \mathbb{1}^{\mathrm{A_0}}\otimes M^{\mathrm{B_0}}_{b,e} \quad \forall b,e, \\
& \sum_b M^{\mathrm{A_0B_0}}_{a,b,e} = M^{\mathrm{A_0}}_{a,e}\otimes\mathbb{1}^{\mathrm{B_0}} \quad \forall a,e; \\
& \sum_b M^{\mathrm{B_0}}_{b,e} = p(e)\mathbb{1}^{\mathrm{B_0}} \quad \forall e, \\
& \sum_a M^{\mathrm{A_0}}_{a,e} = p(e)\mathbb{1}^{\mathrm{A_0}} \quad \forall e, \\
& \sum_e p(e) = 1.
\end{aligned}
\tag{6.36}
$$

The objective function is the total probability for Eve to guess Alice's and Bob's outputs for some specific pair of quantum inputs $\omega^{A_0}_{x^*}$ and $\omega^{B_0}_{y^*}$. The first constraint imposes consistency with the observed behaviour in the experiment, while the remaining constraints ensure a valid effective POVM (which is normalized and no-signalling).

As an example this program can be used to obtain the optimal guessing probability compatible with the probability distribution which arises by Alice and Bob performing Bell state measurements on a shared Werner state $|\Psi\rangle\langle\Psi| = w|\Phi^+\rangle\langle\Phi^+| + (1-w)\frac{\mathbb{1}}{4}$ and with quantum inputs corresponding to the vertices of tetrahedron on the Bloch sphere. The resulting guessing probability in terms of parameter w is given presented in Fig. 6.1.

The correlations obtained on the maximally entangled state ($w = 1$) allow to extract four bits of randomness, because the guessing probability is $\frac{1}{16}$. As in Ref. [CB15] some randomness can be observed from all entangled Werner states, even those admitting a local model. What may be particularly surprising is that actually all Werner states except for the maximally mixed state manifest some randomness. As commented earlier, intuitively this can be explained by the fact that Eve cannot with certainty guess which quantum input was used, which makes the probability distribution random even when there is no entanglement at all.

6.5 Discussion

In this section we have provided new insights into entanglement and randomness detection and quantification in the measurement-device-independent scenario. As explained,

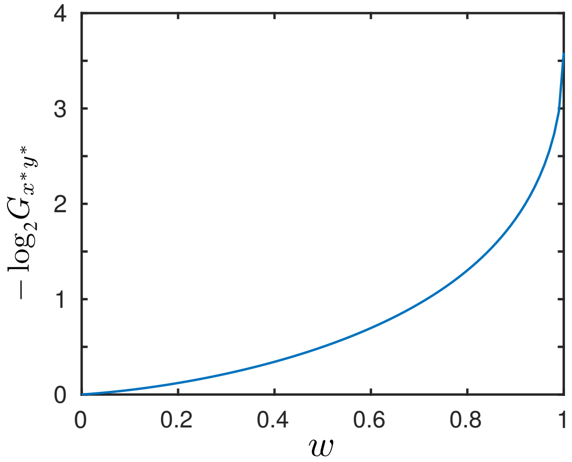

Figure 6.1: Min-entropy ($-\log G_{x^*y^*}$) versus noise w for the probability distribution that arises by performing Bell state measurements on the two-qubit Werner state, and quantum inputs along the vertices of a tetrahedron on the Bloch sphere. For all $w \neq 0$ (i.e. whenever the state is not equal to the maximally mixed state), then randomness can be certified.

this scenario differs from the well-known device-independent scenario by the fact that parties possess a characterized device that can prepare quantum system in some defined quantum states. The scenario in which some parties do not trust their sources and measurements but have a characterized preparation device is not so uncommon in quantum information processing and has been used for constructing protocols for quantum key distribution [LCQ12, BP12] and universal blind quantum computation [BFK09]. In particular, we showed how one can estimate the values of two widely used entanglement measures, robustness-based quantifiers of entanglement, and entanglement negativity. Furthermore we showed how entanglement detection and quantification can be performed in quantum networks (i.e. in situations involving multiple parties, not just two).

On the other hand we showed how possessing a characterized preparation device can decrease adversarial power in guessing measurement outputs. Already a single party which can prepare specific states and measure them with a black box can extract two bits of randomness. Two parties sharing some quantum state can extract randomness even when they do not share any entanglement.

There are a number of interesting directions for future work. First is to study whether the results presented here for the measurement-device-independent scenario can be adapted to other device-independent scenarios. A second interesting avenue is to explore the prospects with regard to full quantum state recovery. A third direction is to focus on mixed quantum inputs – in which can one can imagine that the eavesdropper holds a purification. It is interesting to ask how this affects entanglement detection, and randomness estimation.

Chapter 7

Certifying non-classical teleportation

While the teleportation of physical objects remains an unlikely endeavour present only in science fiction, the teleportation of quantum states stands as one of the cornerstones of quantum information theory. The seminal work by Bennett et al [Ben+93] from 1993 demonstrated the possibility to faithfully transfer the quantum state of a system onto another, spatially distant one. Named quantum teleportation, this protocol made a huge impact on the development of quantum information processing, being a building block for more advanced protocols such as cryptographic tasks [GRTZ02], quantum repeaters [BDCZ98], quantum computing [GC99, RB01] and many others. It has also been experimentally demonstrated in a variety of different systems [Bos+98, Bow+97, Fur+98]. In this chapter we explore teleportation in the context of nonlocal correlations (Section 7.5), provide a simple way to certify (Sections 7.2 and 7.4) and quantify (Section 7.3) teleportation and show that every entangled state can lead to a teleportation experiment which cannot be simulated classically.

7.1 Introduction and classical teleportation

Ideally, in order to realize teleportation, two parties, Alice and Bob, need to share a pair of particles in a maximally entangled state $|\Phi^+\rangle = \sum_{i=0}^{d-1} |ii\rangle / \sqrt{d}$, where d is the local Hilbert space dimension of the system. Then, Alice applies a joint Bell state measurement (a measurement where all measurement operators are maximally entangled) on a third system in state $|\omega\rangle$ and her share of the maximally entangled state and communicates the result to Bob. Bob, upon receiving the message from Alice, applies a unitary operation on his system, which ends up in the desired state $|\omega\rangle$. A very important feature of quantum teleportation is that Alice does not need to know which state she is teleporting to Bob. A similar protocol in which Alice has knowledge of the state to be transferred is known as

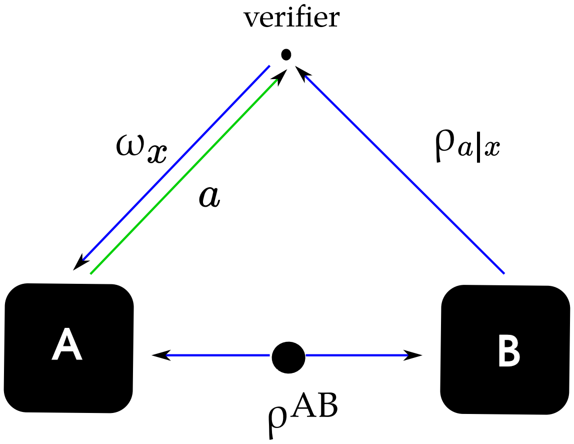

Figure 7.1: Teleportation scenario: Alice and Bob share a bipartite state ρ^{AB}. A verifier, who wants to check whether this state is entangled, sends systems in one of the states ω_x^{V} to Alice, and asks her to transmit it to Bob. Alice applies a global measurement on the state given to her by the verifier and her share of ρ^{AB}, which produces the states $\rho^{\mathrm{B}}_{a|\omega_x}$ for Bob. The verifier has to determine if ρ^{AB} is entangled based on the knowledge of $\{\omega_x^{\mathrm{V}}\}_x$ and $\{\rho^{\mathrm{B}}_{a|\omega_x}\}_{a,x}$.

the remote state preparation [Pat00, Ben+01]. The protocol can be stated without need for Bob to implement the correcting unitaries. In this case there is a third party, called verifier, who sends the states to be teleported to Alice via a quantum channel. Bob uses another quantum channel to send the final state he has to the verifier (see Fig. 7.1). The success of the protocol is estimated by the verifier who simply compares the states obtained by Bob to the states sent to Alice. Before the protocol starts Alice knows that the verifier will send her one of the states from some previously established set, $\{\omega_x\}_x, \omega_x \in \mathbb{B}(\mathscr{H}^{\mathrm{V}})$, which we will call the set of *input states*. The set of states Bob has at the end of the protocol will be named the set of *output states*.

Witnessing non-classical teleportation

In realistic conditions it is impossible to achieve perfect quantum teleportation. There has been a lot of effort in describing imperfect teleportation as well as the role of generic entangled states in the protocol. In a teleportation experiment where a set of states $\{\omega_x\}_x$ – which need not necessarily be pure states – is teleported, the most common benchmark between classical and quantum teleportation is the average fidelity of teleportation

$$\overline{F}_{\sigma_{a|\omega_x}} = \frac{1}{|x|}\sum_{a,x} p(a|\omega_x) F(U_a \rho^{\mathrm{B}}_{a|\omega_x} U_a^\dagger, \omega_x) \tag{7.1}$$

where $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$ is the fidelity, and

$$\rho^{\mathrm{B}}_{a|\omega_x} = \frac{\mathrm{tr}_{\mathrm{VA}}[(M_a^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}})(\omega_x^{\mathrm{V}} \otimes \rho^{\mathrm{AB}})]}{p(a|\omega_x)} \tag{7.2}$$

is the state Bob obtains, conditioned on the input state ω_x and Alice's measurement output a, while $p(a|\omega_x)$ is the probability for Alice to obtain the outcome a when the input state is ω_x. The teleportation process is considered to be quantum (*i.e.* non-classical) if the fidelity of teleportation is higher than the fidelity that could be obtained using solely classical resources (*i.e.* no entanglement pre-shared between Alice and Bob). Based on this figure of merit, not all entangled states are useful for achieving non-classical teleportation, among them the bound entangled states [HHH99].

7.2 Characterization of non-classical teleportation as a SDP optimization

While the benchmark based on the fidelity is widely used to certify non-classical teleportation, one may argue that it is suboptimal to characterize the whole experiment with a single number. Indeed, the verifier has control of sending the input states to Alice and keeps track of the corresponding output states returned by Bob, which, in principle, bears more information than the average fidelity between these two sets of states. Anticipating the optimal characterization, let us recognize a *teleportation channel* mapping each element from the set of input states $\{\omega_x\}_x$ to the classical label a and the corresponding output state $\rho_{a|\omega_x}$. In this section we present a new method to estimate non-classicality of a teleportation experiment by looking for a classical model which could simulate the performance of the corresponding teleportation channel.

Sub-normalized outputs states of Bob are given by

$$\sigma_{a|\omega_x} = \mathrm{tr}_{\mathrm{VA}}[(M_a^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}})(\omega_x{}^{\mathrm{V}} \otimes \rho^{\mathrm{AB}})],$$

where M_a^{VA} are the operators describing the measurement happening inside Alice's box Analogously to the terminology in EPR-steering let us call the set of sub-normalized output states $\{\sigma_{a|\omega_x}\}_{a,x}$ a *teleportation assemblage.* Its elements can alternatively be written as

$$\sigma_{a|\omega_x} = \mathrm{tr}_{\mathrm{A}}[(M_a^{\mathrm{VB}}(\omega_x{}^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}})], \tag{7.3}$$

where

$$M_a^{\mathrm{VB}} = \mathrm{tr}_{\mathrm{A}}\left[(M_a^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}})(\mathbb{1}^{\mathrm{V}} \otimes \rho^{\mathrm{AB}})\right] \tag{7.4}$$

is the so-called *channel operator*, since from Eq. (7.3) we see that it completely characterizes the teleportation channel mapping $\{\omega_x\}$ to $\{\sigma_{a|\omega_x}\}_{a,x}$. Let us inspect the form of the channel operator when Alice and Bob share a separable state, i.e. when $\rho^{\mathrm{AB}} = \sum_\lambda p_\lambda \rho^{\mathrm{A}}_\lambda \otimes \rho^{\mathrm{B}}_\lambda$:

$$\begin{aligned} M_a^{\mathrm{VB}} &= \sum_\lambda p_\lambda \operatorname{tr}_{\mathrm{A}} \left[(M_a^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}})(\mathbb{1}^{\mathrm{V}} \otimes \rho^{\mathrm{A}}_\lambda \otimes \rho^{\mathrm{B}}_\lambda) \right] \\ &= \sum_\lambda p_\lambda \operatorname{tr}_{\mathrm{A}} \left[M_a^{\mathrm{VA}} (\mathbb{1}^{\mathrm{V}} \otimes \rho^{\mathrm{A}}_\lambda) \right] \otimes \rho^{\mathrm{B}}_\lambda . \end{aligned} \tag{7.5}$$

We see that a separable shared state leads to the separable channel operators. On the other hand we can consider the case where the measurement applied by Alice is separable, *i.e.* where $M^{\mathrm{VA}} = \sum_\lambda Q^{\mathrm{V}}_{a,\lambda} \otimes R^{\mathrm{A}}_{a,\lambda}$, for all a and Alice and Bob share any entangled state ρ^{AB}. In this case the channel operator is again separable

$$\begin{aligned} M_a^{\mathrm{VB}} &= \sum_\lambda \operatorname{tr}_{\mathrm{A}} \left[(Q^{\mathrm{V}}_{a,\lambda} \otimes R^{\mathrm{A}}_{a,\lambda} \otimes \mathbb{1}^{\mathrm{B}})(\mathbb{1}^{\mathrm{V}} \otimes \rho^{\mathrm{AB}}) \right] \\ &= \sum_\lambda Q^{\mathrm{V}}_{a,\lambda} \otimes \operatorname{tr}_{\mathrm{A}} \left[(R^{\mathrm{A}}_{a,\lambda} \otimes \mathbb{1}^{\mathrm{B}}) \rho^{\mathrm{AB}} \right] . \end{aligned} \tag{7.6}$$

The insight that classical resources lead to separable channel operators allows formulating the certification of a non-classical teleportation as a conic optimization problem:

$$\begin{aligned} \text{given} \quad & \{\sigma_{a|\omega_x}\}_{a,x}, \{\omega^{\mathrm{V}}_x\}_x \\ \text{find} \quad & M_a^{\mathrm{VB}} \\ \text{s.t.} \quad & \sigma_{a|\omega_x} = \operatorname{tr}[M_a^{\mathrm{VB}} (\omega^{\mathrm{V}}_x \otimes \mathbb{1}^{\mathrm{B}})] \quad \forall a, x, \\ & M_a^{\mathrm{VB}} \in \mathscr{S}, \end{aligned} \tag{7.7}$$

where $\mathscr{S}$ denotes the set of separable operators, i.e. operators of the form $\sum_\lambda Y_\lambda \otimes Z_\lambda$, with $Y_\lambda \geq 0$ and $Z_\lambda \geq 0$ for all λ. Apart from the simple case of 2×2 systems, this set has a complicated structure. However, in general we can consider the set of k-shareable operators as a superset of separable operators, which does have a simpler structure. In particular, by considering this set, the above conic problem becomes an SDP, which can then be solved using standard software packages.

All entangled states demonstrate non-classical teleportation

The observation that classical resources lead to separable channel operators allows to make some further interesting insights about the relation between teleportation and entanglement. Let us assume that Alice applies a Bell state measurement $M_a^{\mathrm{VA}} = (U_a \otimes \mathbb{1}) |\Phi_+\rangle\langle\Phi_+| (U_a^{-1} \otimes \mathbb{1})$, where U_a are the unitaries shifting between different Bell states.

In that case the channel operator has the following form

$$\begin{aligned}
M_a^{\mathrm{VB}} &= \mathrm{tr}_{\mathrm{A}}\left[\left(M_a^{\mathrm{VA}}\otimes \mathbb{1}^{\mathrm{B}}\right)\left(\mathbb{1}^{\mathrm{V}}\otimes\rho^{\mathrm{AB}}\right)\right] \qquad (7.8)\\
&= \mathrm{tr}_{\mathrm{A}}\left\{\left[\left(U_a\otimes\mathbb{1}\right)|\Phi_+\rangle\langle\Phi_+|\left(U_a^{-1}\otimes\mathbb{1}\right)\otimes\mathbb{1}^{\mathrm{B}}\right]\left(\mathbb{1}^{\mathrm{V}}\otimes\rho^{\mathrm{AB}}\right)\right\}\\
&= \frac{1}{d_{\mathrm{VA}}}\mathrm{tr}_{\mathrm{A}}[\mathbb{1}^{\mathrm{A}}\otimes(U_a\otimes\mathbb{1})\rho^{\mathrm{VB}}(U_a^{-1}\otimes\mathbb{1})]\\
&= \frac{1}{d_{\mathrm{VA}}}(U_a\otimes\mathbb{1})\rho^{\mathrm{VB}}(U_a^{-1}\otimes\mathbb{1}),
\end{aligned}$$

where $\rho^{\mathrm{VB}} = \rho^{\mathrm{AB}}$ and d_{VA} is the product of the dimensions of $\mathscr{H}^{\mathrm{V}}$ and $\mathscr{H}^{\mathrm{A}}$. This means that if ρ^{AB} is entangled, then M_a^{VB} will also be entangled for all a. Furthermore, from Eq. (7.3) we see that if the set of input states $\{\omega_x\}_x$ is tomographically complete it is possible to use it to perform quantum process tomography, learn the exact form of operators M_a^{VB} and use any available criterion to estimate its entanglement. Hence, if the set of input states is tomographically complete and Alice applies the Bell state measurement every entangled state she shares with Bob will lead to an entangled channel operator M_a^{VB}. This is in a sharp contrast with the fidelity benchmark, according to which, as we noted earlier, not all entangled states can be used to produce non-classical teleportation.

7.3 Quantifying teleportation

After defining non-classical teleportation as one which cannot be simulated with classical resources and providing the means to certify it, it is interesting to understand how it can be quantified. Basically, the aim is to answer the question of how to say which one of two given experiments demonstrating non-classical teleportation is more non-classical? Quantifying some non-classical property is a very common problem in quantum information theory, examples being quantum coherence [BSP14, MS16, Nap+16], entanglement [PV07], Bell nonlocality [Vic14], EPR-steering [SNC14] and others.

An intuitive way to quantify a property of some non-classical object (entangled state, unsteerable assemblage, non-local probability distribution etc.) is in terms of its robustness to noise. Such robustness measure is expressed as the maximal amount of noise which can be added to the given object before it becomes classical. Specifying the type of added noise allows for different types of robustness to be defined. Entanglement robustness [VT99], introduced in Sec. 2.1.2, can be seen as a prototype for robustness measures of different non-classical resources. Recall that for a bipartite state ρ^{AB} entanglement robustness is defined through the following optimization problem

$$\begin{aligned}
\varepsilon(\rho^{\mathrm{AB}}) &= \min_{r,\rho_s,\sigma_S} r \qquad (7.9)\\
\text{s.t.} \quad & \frac{1}{1+r}\rho^{\mathrm{AB}} + \frac{r}{1+r}\rho_s = \sigma_S\\
& \sigma_S \in \Sigma,
\end{aligned}$$

where Σ denotes the set of separable states. Depending on the properties of ρ_s different types of entanglement robustness can be defined:

- ⋆ *generalized entanglement robustness* [Ste03] ε_{gen}, obtained when the only constraint is that ρ_s is a valid quantum state;
- ⋆ *separable entanglement robustness* ε_{sep}, obtained when the state ρ_s is separable;
- ⋆ *random entanglement robustness* ε_{r}, obtained when the state ρ_s is maximally mixed $\rho_s = \frac{\mathbb{1}}{d^2}$.

Based on the inclusion relations between the sets of states to which ρ_s belongs, it follows

$$\varepsilon_{\text{gen}} \leq \varepsilon_{\text{sep}} \leq \varepsilon_{\text{r}}.$$

Analogously to entanglement robustness it is possible to define teleportation robustness. The central object in a teleportation experiment is the teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$. Robustness of teleportation represents the maximal proportion of a ”noise assemblage” $\{\bar{\sigma}_{a|\omega_x}\}_{a,x}$ with which $\{\sigma_{a|\psi_x}\}_{a,x}$ can be mixed before it becomes classical:

$$\tau(\sigma_{a|\omega_x}) = \max_{r,\{\bar{\sigma}_{a|\omega_x}\}_{a,x}\{M_a^*\}_a} r$$

$$\text{s.t.} \quad \frac{1}{1+r}\sigma^{\text{B}}_{a|\omega_x} + \frac{r}{1+r}\bar{\sigma}^{\text{B}}_{a|\omega_x} = \text{tr}_{\text{V}}[M_a^{*\text{VB}}(\omega_x^{\text{V}} \otimes \mathbb{1}^{\text{B}})], \quad \forall a,x \tag{7.10a}$$

$$\sum_a M_a^{*\text{VB}} = \mathbb{1}^{\text{V}} \otimes \frac{\sum_a \sigma^{\text{B}}_{a|\omega_x} + r\sum_a \bar{\sigma}^{\text{B}}_{a|\omega_x}}{1+r}, \tag{7.10b}$$

$$M_a^{*\text{VB}} \in \mathscr{S} \qquad \forall a. \tag{7.10c}$$

The constrains on the mixing assemblage $\{\bar{\sigma}_{a|\omega_x}\}_{a,x}$ determine different types of teleportation robustness:

- ⋆ *generalized teleportation robustness* τ_{gen}, obtained when the only constraint on the mixing teleportation assemblage is that it is allowed by quantum theory;
- ⋆ *classical teleportation robustness* τ_{cl}, obtained when the mixing teleportation assemblage describes classical teleportation;
- ⋆ *random teleportation robustness* τ_{r}, obtained when each element of the mixing teleportation assemblage is proportional to the maximally mixed state.

In the following subsections we show that each type of teleportation robustness puts a lower bound to the corresponding type of entanglement robustness of the shared state. Moreover, we show that in case Alice applies a full Bell state measurement and the set of input states is tomographically complete each type of teleportation robustness equals the corresponding type of entanglement robustness of the shared state ρ^{AB}.

7.3.1 Lower bounds on entanglement robustness

Entanglement present in the shared state ρ^{AB} is a necessary resource for non-classicality of teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$. With given robustness-based non-classicality measures for both state ρ^{AB} and teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$ it is instructive to compare these two values. Given robustness-based non-classicality measures for both the state ρ^{AB} and the teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$, it is instructive to compare their values.

Generalized teleportation robustness

Let us examine the generalized teleportation robustness of a teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$ obtained by using a measurement $\{M_a\}$ on a shared state ρ^{AB} and a set of input states $\{\omega_x\}_x$. This measure is obtained from (7.10) when the only constraint on $\{\bar{\sigma}_{a|\omega_x}\}_{a,x}$ is that it is admissible by quantum theory:

$$\begin{aligned} \tau_{\mathrm{gen}}(\{\sigma_{a|\omega_x}\}_{a,x}) = & \min_{r,\{M^*_a\}_a,\{\bar{\sigma}_{a|\omega_x}\}_{a,x}} r \\ \text{s.t.} \quad & \frac{\sigma^{\mathrm{B}}_{a|\omega_x} + r\bar{\sigma}^{rB}_{a|\omega_x}}{1+r} = \mathrm{tr}_{\mathrm{V}}\left[M^{*\,\mathrm{VB}}_a(\omega^V_x \otimes \mathbb{1}^{\mathrm{B}})\right]; \\ & \bar{\sigma}^{\mathrm{B}}_{a|\omega_x} \in T_q, \\ & \sum_a M^{*\,\mathrm{VB}}_a = \mathbb{1}^{\mathrm{V}} \otimes \frac{\Sigma_a \sigma_{a|\omega_x} + r\Sigma_a \bar{\sigma}_{a|\omega_x}}{r+1}, \\ & M^{*\,\mathrm{VB}}_a \geq 0, \quad M^{*\,\mathrm{VB}}_a \in \mathscr{S}, \quad \forall a; \end{aligned} \tag{7.11}$$

where T_q is the set of teleportation assemblages admissible by quantum theory. The set of constraints given above imposes that the mixture of the observed assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$ and some other hypothetical assemblage $\{\bar{\sigma}_{a|\omega_x}\}_{a,x}$ can be simulated classically. With an appropriate relaxation of the set of separable operators, all constraints can be written in the linear form and the problem is readily solved by using semidefinite programming optimization (SDP). The only nontrivial constraint regards characterization of the set T_q, but in the next subsection we will show that membership to such set can also be imposed as a semidefinite programming constraint.

Note that the generalized entanglement robustness $\varepsilon_{\mathrm{g}}(\rho^{\mathrm{AB}})$ satisfies

$$\frac{1}{1+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}\rho^{\mathrm{AB}} + \frac{\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}{1+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}\rho_s = \sigma_S \tag{7.12}$$

for a specific quantum state ρ_s and a separable state σ_S. By tensoring with ω^{V}_x and applying the measurement M_a^{VA}, the previous equation becomes

$$\begin{aligned}&\frac{1}{1+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}\operatorname{tr}_{\mathrm{VA}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}}\otimes\rho^{\mathrm{AB}}\right)\right]+\\ &+\frac{\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}{1+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}\operatorname{tr}_{\mathrm{VA}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}}\otimes\rho_s^{\mathrm{AB}}\right)\right]\\ &=\operatorname{tr}_{\mathrm{VA}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}}\otimes\sigma_S^{\mathrm{AB}}\right)\right]\end{aligned}$$

for every x and a. It is equivalent to

$$\frac{1}{1+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}\sigma_{a|\omega_x}+\frac{\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}{1+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}\bar{\sigma}_{a|\omega_x}=\operatorname{tr}_{\mathrm{V}}\left[M_a^{*\mathrm{VB}}\left(\omega_x^{\mathrm{V}}\otimes\mathbb{1}^{\mathrm{B}}\right)\right], \qquad (7.13)$$

where

$$\bar{\sigma}_{a|\omega_x}=\operatorname{tr}_{\mathrm{VA}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}}\otimes\rho_s^{\mathrm{AB}}\right)\right],$$

is a valid teleportation assemblage, while

$$M_a^{*\mathrm{VB}}=\operatorname{tr}_{\mathrm{A}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\mathbb{1}^{\mathrm{V}}\otimes\sigma_S^{\mathrm{AB}}\right)\right] \qquad (7.14)$$

is separable because σ_S is separable. Furthermore, we can write

$$\begin{aligned}\sum_a M_a^{*\mathrm{VB}}&=\operatorname{tr}_{\mathrm{A}}\left[\left(\Sigma_a M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\mathbb{1}^{\mathrm{V}}\otimes\sigma_S^{\mathrm{AB}}\right)\right]\\ &=\operatorname{tr}_{\mathrm{A}}\left(\mathbb{1}^{\mathrm{V}}\otimes\sigma_S^{\mathrm{AB}}\right)\\ &=\mathbb{1}^{\mathrm{V}}\otimes\frac{\operatorname{tr}_{\mathrm{A}}\rho^{\mathrm{AB}}+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})\operatorname{tr}_{\mathrm{A}}\rho_s^{\mathrm{AB}}}{1+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})} \qquad (7.15)\\ &=\mathbb{1}^{\mathrm{V}}\otimes\frac{\Sigma_a\sigma_{a|\omega_x}+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})\Sigma_a\bar{\sigma}_{a|\omega_x}}{1+\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})}\end{aligned}$$

where the second line follows from the completeness relation $\Sigma_a M_a=\mathbb{1}$, the third line follows from Eq. (7.12), and the last line is obtained by using the definitions of $\sigma_{a|\omega_x}$ and $\bar{\sigma}_{a|\omega_x}$. From Eqs. (7.13), (7.15) and separability of $M_a^{*\mathrm{VB}}$ it follows that $\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})$ satisfies all the constraints from (7.11). Since the mixing teleportation assemblage $\bar{\sigma}_{a|\omega_x}$ did not have any special property, besides being realizable in quantum theory, the generalized teleportation robustness of $\{\sigma_{a|\omega_x}\}_{a,x}$ cannot be bigger than $\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}})$:

$$\tau_{\mathrm{gen}}(\sigma_{a|\omega_x})\leq\varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}}). \qquad (7.16)$$

Classical teleportation robustness

Classical teleportation robustness τ_{cl} is defined by (7.10) with the additional constraint that the mixing teleportation assemblage corresponds to classical teleportation. Such a teleportation assemblage is characterized by a positive and separable channel operator $\bar{M}_a^{\mathrm{VB}}$ as shown in Eqs. (7.5) and (7.6). With these constraints the classical teleportation robustness can be obtained from the following optimization problem

$$\begin{aligned}
\tau_{\mathrm{cl}} \quad & (\{\sigma_{a|\omega_x}\}_{a,x}) = \min_{r,\{\bar{M}_a\}_a,\{M^*{}_a\}_a} r \\
\text{s.t.} \quad & \frac{\sigma^{\mathrm{B}}_{a|\omega_x} + r\bar{\sigma}^{\mathrm{B}}_{a|\omega_x}}{1+r} = \mathrm{tr}_{\mathrm{V}}[M^*{}_a{}^{\mathrm{VB}}(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}})]; \\
& \bar{\sigma}^{\mathrm{B}}_{a|\psi_x} = \mathrm{tr}_{\mathrm{V}}\left[\bar{M}_a^{\mathrm{VB}}\left(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}}\right)\right] \quad \forall a,x \\
& \bar{M}_a^{\mathrm{VB}}, M^*{}_a^{\mathrm{VB}} \geq 0, \quad \forall a; \\
& \bar{M}_a^{\mathrm{VB}}, M^*{}_a^{\mathrm{VB}} \in \mathscr{S}, \quad \forall a; \\
& \sum_a \bar{M}_a^{\mathrm{VB}} = \mathbb{1}^{\mathrm{V}} \otimes \Sigma_a \bar{\sigma}_{a|\omega_x}; \\
& \sum_a M^*{}_a^{\mathrm{VB}} = \mathbb{1}^{\mathrm{V}} \otimes \frac{\Sigma_a \sigma_{a|\omega_x} + r\Sigma_a \bar{\sigma}_{a|\omega_x}}{1+r}.
\end{aligned} \tag{7.17}$$

Separability of $\bar{M}_a^{\mathrm{VB}}$ and $M^*{}_a^{\mathrm{VB}}$ cannot be constrained exactly. To solve this issue, the relaxations of the set of separable operators can be used, for example the set of PPT operators or the set of operators admitting k-symmetric extension [DPS02]. The classical teleportation robustness mirrors the separable entanglement robustness, $\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}})$ which satisfies the following equation

$$\frac{1}{1+\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}})}\rho^{\mathrm{AB}} + \frac{\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}})}{1+\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}})}\rho_s = \sigma_S \tag{7.18}$$

where now both states ρ_s and σ_S are separable. By tensoring with ω_x^{V} and applying the measurement M_a^{VA} it becomes

$$\frac{1}{1+\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}})}\sigma_{a|\omega_x} + \frac{\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}})}{1+\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}})}\bar{\sigma}_{a|\omega_x} = \mathrm{tr}_{\mathrm{V}}\left[M_a^{*\mathrm{VB}}\left(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}}\right)\right], \tag{7.19}$$

but now the mixing assemblage can be expressed in terms of separable channel operators $\bar{M}_a^{\mathrm{VB}}$

$$\begin{aligned}
\bar{\sigma}_{a|\psi_x} &= \mathrm{tr}_{\mathrm{V}}\left[\bar{M}_a^{\mathrm{VB}}\left(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}}\right)\right]; \\
\bar{M}_a^{\mathrm{VB}} &= \mathrm{tr}_{\mathrm{A}}\left[\left(M_a^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\mathbb{1}^{\mathrm{V}} \otimes \rho_s^{\mathrm{AB}}\right)\right]; \\
\sum_a \bar{M}_a^{\mathrm{VB}} &= \mathbb{1}^{\mathrm{V}} \otimes \sum_a \bar{\sigma}_{a|\omega_x}
\end{aligned}$$

The channel operators $M_a^{*\mathrm{VB}}$ remain separable and still satisfy relation (7.15). Together with Eqs. (7.19) and separability of $\bar{M}_a^{\mathrm{VB}}$ this implies that $\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}})$ already satisfies all the constraints of the classical teleportation robustness of a teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$ leading to:

$$\tau_{\mathrm{cl}}(\sigma_{a|\omega_x}) \leq \varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}}). \tag{7.20}$$

Random teleportation robustness

The random teleportation robustness was introduced in [CSŠ17], where it is defined as a special case of (7.10) with the additional constraint $\bar{\sigma}_{a|\omega_x} = \frac{1}{|o|}\frac{\mathbb{1}}{d}$, where $|o|$ is the number of outcomes of Alice's measurement. Here we consider a more general version defined as the solution to the following optimization problem

$$\begin{aligned} \tau_{\mathrm{r}} = & \min_{r,\{p(a),M_a^*\}_a} \quad r \\ \text{s.t.} \quad & \frac{\sigma^{\mathrm{B}}_{a|\omega_x} + rp(a)\frac{\mathbb{1}^{\mathrm{B}}}{d}}{1+r} = \mathrm{tr}_{\mathrm{V}}[M_a^{*\mathrm{VB}}(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}})], \qquad \forall a,x \\ & \sum_a p(a) = 1, \quad M_a^{*\mathrm{VB}} \geq 0, \quad M_a^{*\mathrm{VB}} \in \mathscr{S} \qquad \forall a \\ & \sum_a M_a^{*\mathrm{VB}} = \mathbb{1}^{\mathrm{V}} \otimes \frac{\rho^{\mathrm{B}} + r\frac{\mathbb{1}^{\mathrm{B}}}{d}}{1+r}. \end{aligned} \tag{7.21}$$

Let us start from the equation satisfied by random entanglement robustness $\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})$

$$\frac{1}{1+\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})}\rho^{\mathrm{AB}} + \frac{\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})}{1+\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})}\frac{\mathbb{1}}{d^2} = \sigma_S. \tag{7.22}$$

Analogously to the previous cases this equation implies

$$\frac{1}{1+\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})}\sigma^{\mathrm{B}}_{a|\omega_x} + \frac{\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})}{1+\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})}p(a)\frac{\mathbb{1}}{d} = \mathrm{tr}_V[M_a^{*\mathrm{VB}}(\omega_x^V \otimes \mathbb{1}^B)],$$

where

$$p(a) = \mathrm{tr}\left[M_a^{\mathrm{VA}}\left(\omega_x^{\mathrm{V}} \otimes \frac{\mathbb{1}^A}{d}\right)\right] \tag{7.23}$$

and $M_a^{*\mathrm{VB}}$ satisfies Eqs. (7.14) and (7.15) when $\Sigma_a \bar{\sigma}_{a|\omega_x} = \frac{\mathbb{1}}{d}$. Note that (7.23) confirms that $\Sigma_a p(a) = 1$. We have confirmed that $\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})$ satisfies all the constraints from (7.21), thus presenting an upper bound to the random teleportation robustness

$$\tau_{\mathrm{r}}(\sigma_{a|\omega_x}) \leq \varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}}). \tag{7.24}$$

7.3.2 Equivalence between teleportation robustness and entanglement robustness

Following the comparison of teleportation and entanglement quantifiers, in this section we prove that the entanglement robustness of ρ^{AB} is proportional to the corresponding teleportation robustness of $\{\sigma_{a|\omega_x}\}_{a,x}$ in case Alice applies (full or partial) Bell state measurement and has access to a tomographically complete set of input states $\Omega = \{\omega_x\}_x$.

Before considering each type of teleportation robustness separately, let us give in advance the proofs for two auxiliary statements, which will be repeatedly used throughout the remaining part of this section.

Lemma 9.4. *Every element of a teleportation assemblage* $\{\sigma_{a|\omega_x}\}_{a,x}$ *resulting from an arbitrary measurement* M_a^{VA} *and a shared state* ρ^{AB} *could have also been obtained, up to a multiplicative factor, by using as a measurement* $\Phi^{+\mathrm{VA}} = |\Phi^+\rangle\langle\Phi^+|^{\mathrm{VA}}$ *and some other state* $\rho_a'^{\mathrm{AB}}$.

Proof. The identity

$$\mathrm{tr}_{\mathrm{B}}\left[\left(\mathbb{1}^{\mathrm{A}} \otimes M^{\mathrm{BC}}\right)\left(\Phi^{+\mathrm{AB}} \otimes \mathbb{1}^{\mathrm{C}}\right)\right] = \frac{1}{d}\left(M^{\mathrm{AC}}\right)^{T_{\mathrm{A}}}. \tag{7.25}$$

allows us to write any member of a teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$ in the following way

$$\begin{aligned}\sigma^{\mathrm{B}}_{a|\omega_x} &= \mathrm{tr}_{\mathrm{VA}}\left[(M_a^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}})(\omega_x^{\mathrm{V}} \otimes \rho^{\mathrm{AB}})\right] \\ &= d\,\mathrm{tr}_{\mathrm{VV_1A}}\left[\left((\omega_x^{\mathrm{V}})^T \otimes M_a^{\mathrm{V_1A}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\Phi^{+\mathrm{VV_1}} \otimes \rho^{\mathrm{AB}}\right)\right] \\ &= d\,\mathrm{tr}_{\mathrm{VV_1A}}\left[\left(\omega_x^{\mathrm{V}})^T \otimes \mathbb{1}^{\mathrm{V_1AB}}\right)\left(\mathbb{1}^{\mathrm{V}} \otimes M_a^{\mathrm{V_1A}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\Phi^{+\mathrm{VV_1}} \otimes \rho^{\mathrm{AB}}\right)\right]\end{aligned} \tag{7.26}$$

In case $M_a^{\mathrm{V_1A}} = \Phi^{+\mathrm{V_1A}}$ the previous equation reduces to:

$$\sigma^{\mathrm{B}}_{a|\omega_x} = \frac{1}{d}\mathrm{tr}_{\mathrm{V}}\left[\left((\omega_x^{\mathrm{V}})^T \otimes \mathbb{1}^{B}\right)\rho^{\mathrm{VB}}\right]$$

On the other side, if $M_a^{\mathrm{V_1A}}$ is not a Bell state measurement, Eq. (7.26) reduces to

$$\begin{aligned}\sigma^{\mathrm{B}}_{a|\omega_x} &= d\,\mathrm{tr}_{\mathrm{VV_1}}\left[\left(\omega_x^{\mathrm{V}})^T \otimes \mathbb{1}^{\mathrm{V_1AB}}\right)\rho_a'^{\mathrm{VV_1AB}}\right] \\ &= d\,p(a)\,\mathrm{tr}_{\mathrm{V}}\left[\left((\omega_x^{\mathrm{V}})^T \otimes \mathbb{1}^{\mathrm{B}}\right)\rho_a'^{\mathrm{VB}}\right],\end{aligned} \tag{7.27}$$

where

$$p(a) = \mathrm{tr}\left[\left(\mathbb{1}^{\mathrm{V}} \otimes M_a^{\mathrm{V_1A}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\Phi^{+\mathrm{VV_1}} \otimes \rho^{\mathrm{AB}}\right)\right], \tag{7.28}$$

and

$$\rho_a'^{\mathrm{VB}} = \frac{1}{p(a)}\mathrm{tr}_{\mathrm{V_1A}}\left(\mathbb{1}^{\mathrm{V}} \otimes M_a^{\mathrm{V_1A}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\Phi^{+\mathrm{VV_1}} \otimes \rho^{\mathrm{AB}}\right).$$

The state $\rho_a'^{\mathrm{VB}}$ can be obtained from the state ρ^{AB} through a stochastic local operation, which can be seen as a local version of entanglement swapping. To get ρ_a' from ρ Alice uses two auxiliary systems in the maximally entangled state, and applies measurement M_a on one auxiliary system and her share of the state ρ^{AB}. After the measurement she discards the measured systems. Finally, the expression given in Eq. (7.27) can be written as:

$$\begin{aligned}
\sigma^{\mathrm{B}}_{a|\omega_x} &= d^2 p(a) \mathrm{tr}_{\mathrm{VA}}\Big[\left(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{AB}}\right) \left(\Phi^{+\,\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}}\right) \left(\mathbb{1}^{\mathrm{V}} \otimes {\rho'}^{\mathrm{AB}}_a\right) \Big] \\
&= d^2 p(a) \mathrm{tr}_{\mathrm{VA}} \Big[(\Phi^{+\,\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}})(\omega_x^{\mathrm{V}} \otimes {\rho'}^{\mathrm{AB}}_a) \Big], \qquad (7.29)
\end{aligned}$$

which proves Lemma 9.4. The multiplicative factor, mentioned in the statement, is equal to $d^2 p(a)$. □

The assumption that Alice applies a Bell state measurement implicitly bounds the dimension of Alice's reduced state $\rho^{\mathrm{A}} = \mathrm{tr}_{\mathrm{B}}(\rho^{\mathrm{AB}})$ to be equal to the dimension of the input states d. For a general case, d_{A} can be different from d and in Eqs. (7.26-7.29) there is no assumption about d_{A}.

Generalized teleportation robustness

Let us denote by τ^*_{gen} the generalized teleportation robustness of a teleportation assemblage obtained when Alice performs a Bell state measurement $\{M_a^{VA}\}_a$ and the set of input states $\Omega = \{\omega_x\}_x$ is tomographically complete. In this case the first constraint from (7.11) can be rewritten as

$$\begin{aligned}
& \frac{1}{1+r}\sigma^{\mathrm{B}}_{a|\omega_x} + \frac{r}{1+r}\bar{\sigma}^{\mathrm{B}}_{a|\omega_x} = \qquad (7.30) \\
=\ & \frac{1}{r+1}\mathrm{tr}_{\mathrm{VA}}\left[\left(U_a^{\mathrm{A}} \Phi^{+\,\mathrm{VA}} U_a^{\dagger\,\mathrm{A}} \otimes \mathbb{1}^{\mathrm{B}} \right) \left(\omega_x^{\mathrm{V}} \otimes \rho^{\mathrm{AB}} \right) \right] + \\
& + \frac{1}{r+1}\mathrm{tr}_{\mathrm{VA}}\left[\left(\Phi^{+\,\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}} \right) \left(\omega_x^{\mathrm{V}} \otimes d^2 p(a) {\rho'}^{\mathrm{AB}}_a \right) \right] \\
=\ & \frac{1}{d}\mathrm{tr}_{\mathrm{V}}\left[\left(\frac{U_a^{\mathrm{V}} \rho^{\mathrm{VB}} U_a^{\dagger\,\mathrm{V}} + r d^2 p(a) {\rho'}^{\mathrm{VB}}_a}{r+1} \right)^{T_{\mathrm{V}}} \left(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}} \right) \right] \\
=\ & \mathrm{tr}_{\mathrm{V}}[{M^*_a}^{\mathrm{VB}} (\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}})].
\end{aligned}$$

The second line comes from the assumption that Alice applies a Bell state measurement and U_a are local unitary transformations shifting between different Bell states $M_a = U_a \Phi^+ U_a^\dagger$. The third line uses a way to characterize a general teleportation assemblage $\{\bar{\sigma}_{a|\omega_x}\}_{a,x}$ given in Lemma 9.4, with the specific constraint given in Eq. (7.29). To get the fourth line we used the identity (7.25). Given that the set of quantum inputs Ω is tomographically complete the last equality imposes

$${M^*_a}^{\mathrm{VB}} = \frac{1}{d}\left(\frac{1}{r+1} U_a^{\mathrm{V}} \rho^{\mathrm{VB}} U_a^{\dagger\,\mathrm{V}} + \frac{r}{1+r} d^2 p(a) {\rho'}^{\mathrm{VB}}_a \right)^{T_{\mathrm{V}}} \qquad (7.31)$$

With this in mind we can once more rewrite the optimization problem (7.11):

$$\begin{aligned}
\tau^*_{\text{gen}}(\sigma_{a|\omega_x}) = & \min_{\{r_a, M^*_a, p(a), \rho'_a\}_a} r \\
\text{s.t.} \quad & \frac{1}{r+1} U^{\text{V}}_a \rho^{\text{VB}} U^{\dagger\text{V}}_a + \frac{r}{1+r} d^2 p(a) {\rho'}^{\text{VB}}_a = d \left(M^{*\text{VB}}_a \right)^{T_{\text{V}}}; && (7.32\text{a}) \\
& M^{*\text{VB}}_a \geq 0, \quad M^{*\text{VB}}_a \in \mathscr{S} \quad \forall a; && (7.32\text{b}) \\
& \sum_a p(a) {\rho'}^{\text{VB}}_a = \frac{\mathbb{1}^{\text{V}}}{d} \otimes \rho'^{\text{B}}, \quad \sum_a p(a) = 1, && (7.32\text{c}) \\
& \sum_a M^{*\text{VB}}_a = 1^{\text{V}} \otimes \frac{\rho^{\text{B}} + r\rho'^{\text{B}}}{1+r}, && (7.32\text{d})
\end{aligned}$$

which resembles the optimization problem defining the generalized entanglement robustness of the state $\rho^{\text{VB}} = \rho^{\text{AB}}$. Indeed the optimization problem (7.32) taken for one specific value of a, say $a = 0$, for which $U_0 = \mathbb{1}$ is similar to (7.9), the difference being that $d^2 p(a) \rho'_a$ and dM^{*VB}_a are not necessarily normalized and the added constraints (7.32c) and (7.32d). The constraint (7.32a) for $a = 0$ has a solution if $d \operatorname{tr} M^{*\text{VB}}_0 = (1 + rd^2 p(0))/(1+r)$. Taking this into account, the constraint can be rearranged in the following way

$$\frac{\rho^{\text{VB}} + rd^2 p(0) {\rho'_0}^{\text{VB}}}{1 + rd^2 p(0)} = \frac{1}{\operatorname{tr} M^{*\text{VB}}_0} \left(M^{*\text{VB}}_0 \right)^{T_{\text{V}}}, \tag{7.33}$$

which is now equivalent to the first constraint from (7.9). Thus, the minimal r satisfying this constraint for separable $M^{*\text{VB}}_0$ is equal to $\varepsilon_{\text{gen}}(\rho^{\text{AB}})/(d^2 p(0))$. In a similar manner the minimal r satisfying (7.32a) for $a \neq 0$ and separable $M^{*\text{VB}}_a$ is equal to $\varepsilon_{\text{gen}}(\rho^{\text{AB}})/(d^2 p(a))$ because the generalized entanglement robustness is the same for all the states which are mutually related by a local unitary transformation. Let us, for a moment, suppose that there is at least one a such that $d^2 p(a) \geq 1$. Since there are d^2 different values of a, Eq. (7.32c) implies that for some other value of a, say $a = a'$ it must be $d^2 p(a') \leq 1$. But in this case the smallest r satisfying constraints (7.32a) and (7.32b) for all a must be strictly bigger than $\varepsilon_{\text{gen}}(\rho^{AB})$. On the other side, if $d^2 p(a) = 1$ for all values of a, the smallest r satisfying (7.32) is exactly equal to $\varepsilon_{\text{gen}}(\rho^{\text{AB}})$. Since $p(a)$ are optimization variables the minimal τ_{gen} will be achieved when all $p(a)$s are equal.

Finally, we have to make sure that constraints (7.32c) and (7.32d) are satisfied by the solution $r = \varepsilon_{\text{gen}}(\rho^{\text{VB}})$. If (7.32a) for $a = 0$ is satisfied for some ${\rho'_0}^{\text{VB}}$ and $M^{*\text{VB}}_0$, for $a \neq 0$ it will be satisfied with the same r, ${\rho'_a}^{\text{VB}} = U^{\text{V}}_a {\rho'_0}^{\text{VB}} U^{\dagger\text{V}}_a$ and $M^{*\text{VB}}_a = U^{\text{V}}_a M^{*\text{VB}}_0 U^{\dagger\text{V}}_a$ implying

$$\sum_a p(a) {\rho'_a}^{\text{VB}} = \frac{\mathbb{1}^{\text{V}}}{d} \otimes \rho'^{\text{B}}$$

because $\sum_a U_a^{\mathrm{V}} \rho_a'^{\mathrm{VB}} U_a^{\dagger\mathrm{V}} = d\mathbb{1}^{\mathrm{V}} \otimes \rho'^{\mathrm{B}}$. Validity of (7.32d) is verified by summing (7.32a) over all different values of a:

$$\begin{aligned}\sum_a M_a^{*\mathrm{VB}} &= \frac{1}{d}\sum_a U_a^{\mathrm{V}} \frac{\left(\rho^{\mathrm{VB}}\right)^{T_{\mathrm{V}}} + r\left(\rho_0'^{\mathrm{VB}}\right)^{T_{\mathrm{V}}}}{1+r} U_a^{\dagger\mathrm{V}} \\ &= \mathbb{1}^{\mathrm{V}} \otimes \frac{\rho^{\mathrm{B}} + r\rho'^{\mathrm{B}}}{1+r}.\end{aligned}$$

By establishing the equivalence between the optimization problem (7.11), in case Alice performs a full Bell state measurement on her share of the state and an element from a tomographically complete set of input states, and the one for generalized entanglement robustness we can conclude that

$$\tau^*_{\mathrm{gen}}(\{\sigma_{a|\omega_x}\}_{a,x}) = \varepsilon_{\mathrm{gen}}(\rho^{\mathrm{AB}}). \tag{7.34}$$

Classical teleportation robustness

For the easier comparison let us restate the definition of separable entanglement robustness, which is obtained from (7.9) with the constraint that ρ_s is a separable state

$$\begin{aligned}\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}}) &= \min_{r,\rho_s,\sigma_S} r \\ \text{s.t.} \quad & \frac{1}{1+r}\rho^{\mathrm{AB}} + \frac{r}{1+r}\rho_s = \sigma_S \\ & \rho_s, \sigma_S \in \Sigma,\end{aligned} \tag{7.35}$$

Let us consider the classical teleportation robustness of a teleportation assemblage obtained when Alice applies a full Bell state measurement and uses a tomographically complete set of inputs and denote it by τ^*_{cl}. In order to reduce (7.17) to (7.35), it is useful to switch from variables $\bar{M}_a$ to $p(a)$ and ρ_a' which are related in the following way:

$$dp(a)\left(\rho'^{\mathrm{VB}}_a\right)^{T_{\mathrm{V}}} = \bar{M}_a^{\mathrm{VB}} \tag{7.36}$$

Now, the teleportation assemblage members $\bar{\sigma}^{\mathrm{B}}_{a|\psi_x}$ can be written in the form given in Eq. (7.29).

The simplification used in (7.30) can be again used in exactly the same way to reduce the second line of (7.17) to

$$\begin{aligned}&\mathrm{tr}_{\mathrm{V}}\left[\left(\frac{1}{r+1}U_a^{\mathrm{V}}\rho^{\mathrm{VB}}U_a^{\dagger\mathrm{V}} + \frac{r}{1+r}d^2p(a)\rho_a'^{\mathrm{VB}}\right)^{T_{\mathrm{V}}}\left(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}}\right)\right] \\ &= d\mathrm{tr}_{\mathrm{V}}[M_a^{*\mathrm{VB}}(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}})].\end{aligned} \tag{7.37}$$

Since the set of input states is tomographically complete Eq. (7.37) implies

$$\frac{1}{r+1}U_a^{\mathrm{V}}\rho^{\mathrm{VB}}U_a^{\dagger\mathrm{V}}+\frac{r}{1+r}d^2p(a)\rho_a'^{\mathrm{VB}}=d\left(M_a^{*\mathrm{VB}}\right)^{T_{\mathrm{V}}},$$

but in this case ρ_a' are separable, which is the consequence of (7.36) and the separability of $\bar{M}_a^{\mathrm{VB}}$. Now the optimization (7.17) reduces to

$$\begin{aligned}
&\tau_{\mathrm{cl}}^*(\sigma_{a|\omega_x}) = \min_{r,\{\bar{M}_a,p(a)\rho_a'\}_a} r && (7.38a)\\
\text{s.t.}\quad &\frac{1}{r+1}U_a^{\mathrm{V}}\rho^{\mathrm{VB}}U_a^{\dagger\mathrm{V}}+\frac{r}{1+r}d^2p(a)\rho_a'^{\mathrm{VB}}=d\left(M_a^{*\mathrm{VB}}\right)^{T_{\mathrm{V}}}; && (7.38b)\\
&M_a^{*\mathrm{VB}}\geq 0,\quad M_a^{*\mathrm{VB}}\in\mathscr{S}\quad\forall a; && (7.38c)\\
&\rho_a'^{\mathrm{VB}}\geq 0,\quad \rho_a'^{\mathrm{VB}}\in\Sigma\quad\forall a; && (7.38d)\\
&\sum_a p(a)\rho_a'^{\mathrm{VB}}=\frac{\mathbb{1}^{\mathrm{V}}}{d}\otimes\bar{\rho}^{\mathrm{B}}; && (7.38e)\\
&\sum_a M^*{}_a^{\mathrm{VB}}=\mathbb{1}^{\mathrm{V}}\otimes\frac{\rho^{\mathrm{B}}+r\bar{\rho}^{\mathrm{B}}}{1+r}. && (7.38f)
\end{aligned}$$

In order to emphasize the resemblance with (7.35) let us rewrite (7.38b) in the following way

$$\frac{U_a^{\mathrm{V}}\rho^{\mathrm{VB}}U_a^{\dagger\mathrm{V}}+rd^2p(a)\rho_a'^{\mathrm{VB}}}{1+rd^2p_a}=\frac{1}{\mathrm{tr}M_a^{*\mathrm{VB}}}\left(M_a^{*\mathrm{VB}}\right)^{T_{\mathrm{V}}}.$$

Since all states mutually related by local unitary transformations have the same value of classical entanglement robustness, the smallest r satisfying the last equation for each a is equal to $\varepsilon_{\mathrm{sep}}/d^2p(a)$. Analogously to the case of generalized teleportation robustness the optimal r is obtained when $p(a)=1/d^2$ and $\rho_a'=U_a\rho_0'U_a^\dagger$, for all values of a and is equal to $\varepsilon_{\mathrm{sep}}(\rho^{AB})$, which implies

$$\tau_{\mathrm{cl}}^*(\sigma_{a|\omega_x})=\varepsilon_{\mathrm{sep}}(\rho^{\mathrm{AB}}). \tag{7.39}$$

Random teleportation robustness

Finally, we consider the random teleportation robustness of a teleportation assemblage obtained when Alice applies a full Bell state measurement and uses a tomographically complete set of input states and denote it by τ_{r}^*. Let us compare it to the random entanglement robustness ε_{r}:

$$\begin{aligned}
\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}}) \quad &= \quad \min_{r,\sigma_S}\quad r && (7.40)\\
\text{s.t.}\qquad & \qquad \frac{1}{1+r}\rho^{\mathrm{AB}}+\frac{r}{1+r}\frac{\mathbb{1}}{d^2}=\sigma_S\\
& \qquad \sigma_S\in\Sigma.
\end{aligned}$$

Recall that the definition of the random teleportation robustness of a teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$ is given in (7.21). The first constraint of (7.21) in case Alice applies a Bell state measurement reads

$$\begin{aligned}
&\frac{1}{1+r}\sigma^{\mathrm{B}}_{a|\omega_x}+\frac{r}{1+r}p(a)\frac{\mathbb{1}^{\mathrm{B}}}{d} = \\
= \;& \mathrm{tr}_{\mathrm{VA}}\left[\left(\Phi^{+\,\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}}\otimes\frac{U_a^{\mathrm{A}}\rho^{\mathrm{AB}}U_a^{\dagger\,\mathrm{A}}+rp(a)\mathbb{1}^{\mathrm{AB}}}{1+r}\right)\right] \\
= \;& \frac{1}{d}\mathrm{tr}_{\mathrm{V}}\left[\left(\frac{U_a^{\mathrm{V}}\rho^{\mathrm{VB}}U_a^{\dagger\,\mathrm{V}}+rp(a)\mathbb{1}^{\mathrm{VB}}}{1+r}\right)^{T_{\mathrm{V}}}\left(\omega_x^{\mathrm{V}}\otimes\mathbb{1}^{\mathrm{B}}\right)\right] \qquad (7.41) \\
= \;& \mathrm{tr}_{\mathrm{V}}\left[M_a^{*\,\mathrm{VB}}(\omega_x^{\mathrm{V}}\otimes\mathbb{1}^{\mathrm{B}})\right]
\end{aligned}$$

For a tomographically complete set of inputs this condition is satisfied if and only if

$$\frac{U_a^{\mathrm{V}}\rho^{\mathrm{VB}}U_a^{\dagger\,\mathrm{V}}+rp(a)\mathbb{1}^{\mathrm{AB}}}{1+r}=d\left(M_a^{*\,\mathrm{VB}}\right)^{T_{\mathrm{V}}} \tag{7.42}$$

Following this simplification, Eq. (7.21) reduces to

$$\begin{aligned}
\tau_{\mathrm{r}} = & \min_{r,\{M_a^*,p(a)\}_a} r \\
\text{s.t.} \quad & \frac{U_a^{V}\rho^{\mathrm{VB}}U_a^{\dagger\,\mathrm{V}}+rp(a)\mathbb{1}^{\mathrm{VB}}}{1+r}=d\left(M_a^{*\,\mathrm{VB}}\right)^{T_{\mathrm{V}}} \qquad \forall a,x && (7.43a) \\
& M_a^{*\,\mathrm{VB}}\geq 0, \quad M_a^{*\,\mathrm{VB}}\in\mathscr{S} \qquad \forall a, && (7.43b) \\
& \sum_a M_a^{*\,\mathrm{VB}}=\mathbb{1}\otimes\frac{\rho^{\mathrm{B}}+r\frac{\mathbb{1}^{\mathrm{B}}}{d}}{1+r}. && (7.43c)
\end{aligned}$$

Eq. (7.43a) for every a can be transformed in the following way

$$\frac{U_a^{\mathrm{V}}\rho^{\mathrm{VB}}U_a^{\dagger\,\mathrm{V}}+rd^2p(a)\frac{\mathbb{1}^{\mathrm{AB}}}{d^2}}{1+rd^2p(a)}=\frac{1}{\mathrm{tr}M_a^{*\,\mathrm{VB}}}\left(M_a^{*\,\mathrm{VB}}\right)^{T_{\mathrm{V}}}.$$

Thus, the smallest r satisfying (7.43a) and (7.43b) for each a separately is equal to $\varepsilon_{\mathrm{r}}(U_a^{V}\rho^{\mathrm{VB}}U_a^{\dagger\,\mathrm{V}})/d^2p(a)=\varepsilon_{\mathrm{r}}(\rho^{\mathrm{VB}})/d^2p(a)$. Since there are d^2 different outcomes a, the smallest r which can simultaneously satisfy (7.43a) for all values of a is equal to ε_{r}. By summing (7.42) over a, we get that a constraint equivalent to the one from (7.21) is satisfied, which finally implies

$$\tau_{\mathrm{r}}^*(\sigma_{a|\omega_x})=\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}}).$$

When considering teleportation protocols in which Alice applies a two-outcome measure-

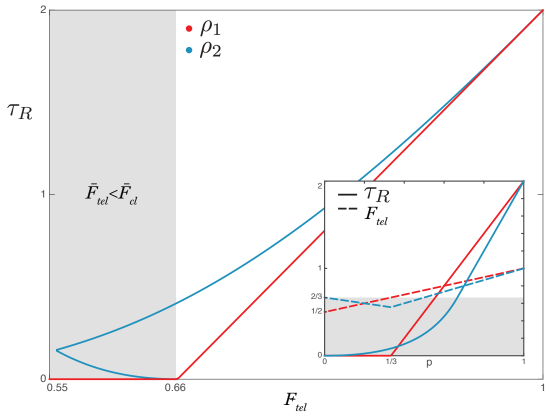

Figure 7.2: Average fidelity of teleportation versus random teleportation robustness for $\rho_1^{\mathrm{AB}} = p|\Phi^+\rangle\langle\Phi^+| + (1-p)\frac{\mathbb{1}^{\mathrm{AB}}}{4}$ (red) and $\rho_2^{\mathrm{AB}} = p|\Phi^+\rangle\langle\Phi^+| + (1-p)|01\rangle\langle 01|$ (blue). The shaded area shows the region where the average fidelity of teleportation is below the classical average fidelity $\bar{F}_{cl} = 2/3$. The inset shows the same quantities as a function of the noise parameter p for the two states. Notice that for the same values of $\overline{F}_{tel}$ the two states give different values for τ_r. This means that, although the two states perform equally as quantified by the average fidelity, when quantified instead by the random teleportation robustness ρ_2^{AB} produces teleportation data which is more non-classical than ρ_1^{AB} does.

ment, the benchmark for success is the situation when Alice performs a partial Bell state measurement using the POVM $M_0^{\mathrm{VA}} = \Phi^{+\mathrm{VA}}$, $M_1^{\mathrm{VA}} = \sum_{i=1}^{d^2-1} U_i^{\mathrm{V}} \Phi^{+\mathrm{VA}} U_i^{\dagger\,\mathrm{V}}$ and has access to a tomographically complete set of input states. Let us the denote random teleportation robustness of a teleportation assemblage obtained by performing such measurement as τ_{r}'. Taking into account that the set of input states is tomographically complete, τ_{r}' can be obtained from the following optimization problem

$$\tau_{\mathrm{r}}' = \min_{r,\{M_a^*, p(a)\}_a} \; r$$

$$\text{s.t.} \quad \frac{\rho^{\mathrm{VB}} + rp(0)\mathbb{1}^{\mathrm{VB}}}{1+r} = d\left(M_0^{*\,\mathrm{VB}}\right)^{T_{\mathrm{V}}}, \tag{7.44a}$$

$$\frac{\sum_{i=1}^{d^2-1} U_i^{\mathrm{V}} \rho^{\mathrm{VB}} U_i^{\dagger\,\mathrm{V}} + rp(1)\mathbb{1}^{\mathrm{VB}}}{1+r} = d\left(M_1^{*\,\mathrm{VB}}\right)^{T_{\mathrm{V}}}, \tag{7.44b}$$

$$M_a^{*\,\mathrm{VB}} \geq 0, \quad M_a^{*\,\mathrm{VB}} \in \mathscr{S} \qquad \forall a, \tag{7.44c}$$

$$\sum_a M_a^{*\,\mathrm{VB}} = \mathbb{1} \otimes \frac{\rho^{\mathrm{B}} + r\frac{\mathbb{1}^{\mathrm{B}}}{d}}{1+r}. \tag{7.44d}$$

Note that constraint (7.44b), based on (7.44a) and satisfying (7.44d) can be reduced to

$$M_1^{*\,\mathrm{VB}} = \sum_{i=1}^{d^2-1} M_0^{*\,\mathrm{VB}} + \frac{\big(p(1) - p(0)(d^2-1)\big)\,\mathbb{1}^{\mathrm{VB}}}{d(1+r)},$$

which is separable whenever $M_0^{*\,\mathrm{VB}}$ is separable[1]. This means that every r satisfying (7.44a) also satisfies (7.44b), which in turn implies that $\tau_{\mathrm{r}}'(\sigma_{a|\omega_x})$ is equal to the smallest r satisfying (7.44a) and (7.44c). Following the equivalence of (7.44) and (7.40), such smallest r is equal to $\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})/d^2 p(0))$. The optimal mixing assemblage is the trivial one $\{\mathbb{1}^{\mathrm{B}}/d, 0\}$ leading to

$$\tau_{\mathrm{r}}'(\sigma_{a|\omega_x}) = \frac{\varepsilon_{\mathrm{r}}(\rho^{\mathrm{AB}})}{d^2}, \tag{7.45}$$

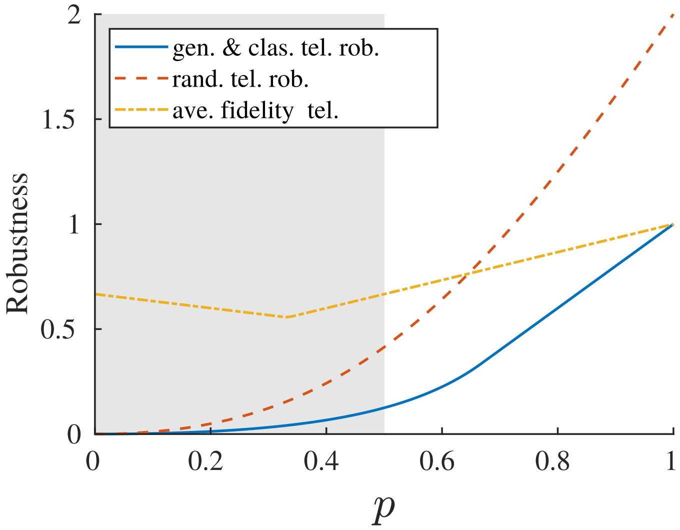

Figure 7.3: Teleportation robustnesses and the average fidelity of teleportation for the state $\rho = p\,|\Phi^+\rangle\langle\Phi^+| + (1-p)\,|01\rangle\langle 01|$. The set of quantum inputs consists of all eigenstates of the three Pauli operators. For this particular teleportation assemblage the generalized and classical teleportation robustness coincide. We can see that even when the average teleportation fidelity is smaller than $2/3$ the robustness quantifiers are larger than zero, demonstrating non-classical teleportation.

7.3.3 Teleportation weight

Another operationally meaningful teleportation quantifier different than robustness is the teleportation weight. Any teleportation assemblage can be written as a convex combination of an assemblage obtained via classical teleportation and a non-classical one. The

[1] This is expected since constraint (7.44b) corresponds to the member of teleportation assemblage which is obtained by using separable measurement M_1^{VA}.

minimal proportion of the non-classical teleportation assemblage defines the teleportation weight. It can be seen as an analogue to the best separable approximation [LS98], steering weight [SNC14], incompatibility weight [Pus15] or recently introduced asymmetry and coherence weight [BNS17]. Mathematically, we define teleportation weight in the following way

$$\begin{aligned} \mathrm{TW}(\sigma^{\mathrm{B}}_{a|\omega_x}) = \min \quad & p \\ \text{s.t.} \quad & \sigma^{\mathrm{B}}_{a|\omega_x} = \mathrm{tr}_{\mathrm{V}}[(p\tilde{M}^{\mathrm{VB}}_a + (1-p)\bar{M}^{\mathrm{VB}}_a)\omega^{\mathrm{V}}_x \otimes \mathbb{1}^{\mathrm{B}}] \\ & \sum_a \mathrm{tr}_{\mathrm{V}}[\tilde{M}^{*\mathrm{VB}}_a(\omega^{\mathrm{V}}_x \otimes \mathbb{1}^{\mathrm{B}})] = \sum_a \mathrm{tr}_{\mathrm{V}}[\tilde{M}^{*\mathrm{VB}}_a(\omega'^{\mathrm{V}}_x \otimes \mathbb{1}^{\mathrm{B}})], \quad \forall x, x', \\ & \bar{M}^{\mathrm{VB}}_a \geq 0, \quad \bar{M}^{\mathrm{VB}}_a \in \mathscr{S}, \quad \forall a, \\ & \left(\tilde{M}^{*\mathrm{VB}}_a\right)^{T_{\mathrm{V}}} \geq 0, \quad \forall a. \end{aligned} \tag{7.46}$$

In this definition the channel operators $\bar{M}^{\mathrm{VB}}_a$ are describing classical teleportation, which is why they have to be positive and separable , while $\tilde{M}^{\mathrm{VB}}_a$ are the channel operators corresponding to non-classical teleportation, satisfying constraint on the positivity of the partial transpose (7.25). A non-zero teleportation weight witnesses that teleportation is non-classical, which in turn means that the state Alice and Bob share is entangled. When the set of input states is tomographically complete and the state Alice and Bob share is maximally entangled the teleportation weight must be equal to 1. Moreover, any pure entangled shared state with tomographically complete set of input states has the maximal teleportation weight.

Just as teleportation robustness quantifiers can be seen to provide bounds on the corresponding entanglement robustness quantifiers, so too does the teleportation weight of the teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$ place a lower bound on the best separable approximation of the state $\rho^{\rangle\mathrm{B}}$. The best separable approximation of a bipartite state $\rho^{\rangle\mathrm{B}}$ is a monotone which says how much of a separable state is contained in the state ρ^{AB} and is defined as

$$\begin{aligned} \varepsilon_{\mathrm{BSA}}(\rho^{\mathrm{AB}}) = \min_{p,\rho_s,\sigma_S} & \; p \\ \text{s.t.} \quad & \rho^{\mathrm{AB}} = p\rho_s + (1-p)\sigma_S, \\ & \sigma_S \in \mathscr{S}, \end{aligned} \tag{7.47}$$

For the state ρ^{AB} and its best separable approximation $\varepsilon_{\mathrm{BSA}}(\rho^{\mathrm{AB}})$ there exist a corresponding quantum state $\tilde{\rho}^{\mathrm{AB}}$ and separable state $\bar{\rho}^{\mathrm{AB}}$ such that

$$\rho^{\mathrm{AB}} = \varepsilon_{\mathrm{BSA}}(\rho^{\mathrm{AB}})\tilde{\rho}^{\mathrm{AB}} + (1 - \varepsilon_{\mathrm{BSA}}(\rho^{\mathrm{AB}}))\bar{\rho}^{\mathrm{AB}}$$

By tensoring ρ^{AB} with the state ω_x^{V} and applying a joint measurement M_a^{VA}, this implies

$$\begin{aligned}\mathrm{tr}_{\mathrm{VA}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}}\otimes\rho^{\mathrm{AB}}\right)\right] = \\ \varepsilon_{\mathrm{BSA}}(\rho^{\mathrm{AB}})\,\mathrm{tr}_{\mathrm{VA}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}}\otimes\tilde{\rho}^{\mathrm{AB}}\right)\right] \\ +\left(1-\varepsilon_{\mathrm{BSA}}(\rho^{\mathrm{AB}})\right)\mathrm{tr}_{\mathrm{VA}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}}\otimes\bar{\rho}^{\mathrm{AB}}\right)\right],\end{aligned}$$

i.e.

$$\sigma^{\mathrm{B}}_{a|\omega_x} = \mathrm{tr}_{\mathrm{V}}\Big[\Big(\varepsilon_{\mathrm{BSA}}(\rho^{\mathrm{AB}})\tilde{M}_a^{\mathrm{VB}} + \left(1-\varepsilon_{\mathrm{BSA}}(\rho^{\mathrm{AB}})\right)\bar{M}_a^{\mathrm{VB}}\Big)\omega_x^{\mathrm{V}}\otimes\mathbb{1}^{\mathrm{B}}\Big], \tag{7.48}$$

where

$$\begin{aligned}\tilde{M}_a^{\mathrm{VB}} &= \mathrm{tr}_{\mathrm{A}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\mathbb{1}^{\mathrm{V}}\otimes\tilde{\rho}^{\mathrm{AB}}\right)\right], \\ \bar{M}_a^{\mathrm{VB}} &= \mathrm{tr}_{\mathrm{A}}\left[\left(M_a^{\mathrm{VA}}\otimes\mathbb{1}^{\mathrm{B}}\right)\left(\mathbb{1}^{\mathrm{V}}\otimes\bar{\rho}^{\mathrm{AB}}\right)\right],\end{aligned} \tag{7.49}$$

for all a and x, (7.48) is equivalent to the first constraint from the optimization problem (7.46). Moreover, the operators $\tilde{M}_a^{\mathrm{VB}}$ and $\bar{M}_a^{\mathrm{VB}}$ defined in (7.49) satisfy all the other constraints from (7.46). Thus, the teleportation weight of the teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$ can only be smaller than the best separable approximation of the shared state ρ^{AB}, i.e.

$$\mathrm{TW}(\{\sigma^{\mathrm{B}}_{a|\omega_x}\}_{a,x}) \leq \varepsilon_{\mathrm{BSA}}(\rho^{\mathrm{AB}}).$$

The teleportation weight of the state $p\,|\Phi^+\rangle\langle\Phi^+| + (1-p)\frac{\mathbb{1}}{4}$ corresponding to different scenarios (*i.e.* different sets of input states) is presented in Fig. 7.4. We see that the teleportation weight for a tomographically complete set of input states is larger than zero whenever $p > \frac{1}{3}$, which is the separability bound for Werner states. This does not change even if Alice does not apply the full Bell state measurements, but projects only onto one of the Bell states (*i.e.* a partial Bell state measurement). When the set of input states consists of eigenstates of two Pauli observables, non-classical teleportation is detected only when $p > \frac{1}{2}$.

One of the most striking new insights resulting from using all the observable data in a teleportation experiment is that all entangled states can be used to certify non-classical teleportation. Previously, all bound entangled states were considered to be useless for teleportation. One of the most famous examples of bound entangled states is the Horodecki

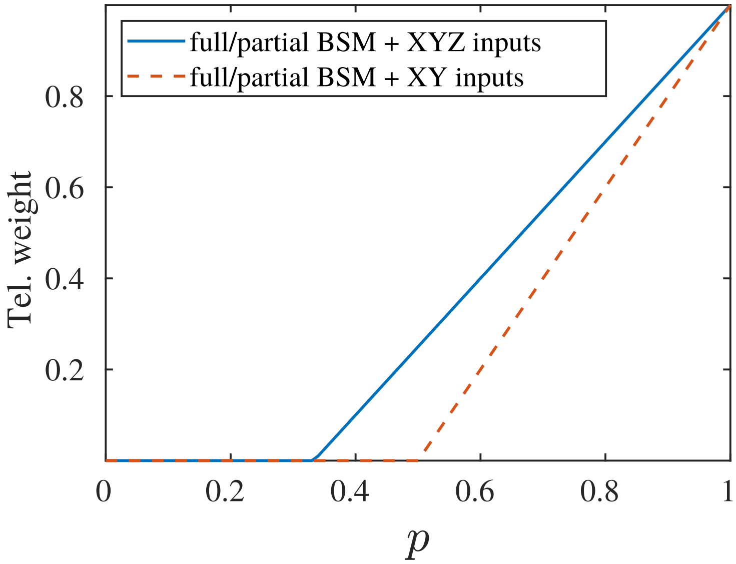

Figure 7.4: Teleportation weight for different scenarios involving the state $p\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + (1-p)\frac{\mathbb{1}}{4}$: Alice either performs a full or partial Bell State Measurement, and uses either a tomographically complete set of inputs (eigenstates of $\sigma_{\rm X}$,$\sigma_{\rm Y}$ and $\sigma_{\rm Z}$), or a tomographically incomplete set of measurements (eigenstates of $\sigma_{\rm X}$ and $\sigma_{\rm Z}$. The teleportation weight is insensitive to the choice of measurements for both sets of inputs, indicating that it is only the conclusive events (corresponding to POVM elements that are entangled) that count.

state [Hor97]:

$$\rho_H = \frac{1}{8a+1}\begin{pmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1+a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & a & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+a}{2} \end{pmatrix}, \tag{7.50}$$

for values $a \in (0,1)$. The dependence of the teleportation weight of the teleportation assemblage obtained by using the Horodecki state with parameter a is given on Fig. 7.5. The set of input states is chosen to be tomographically complete and a partial Bell state measurements is performed ($M_1^{\rm VA} = \left|\Phi^+\right\rangle\left\langle\Phi^+\right|$, $M_2^{\rm VA} = \mathbb{1} - M_1^{\rm VA}$). The teleportation weight of the Horodecki state is small in value, but we observed that other bound entangled states

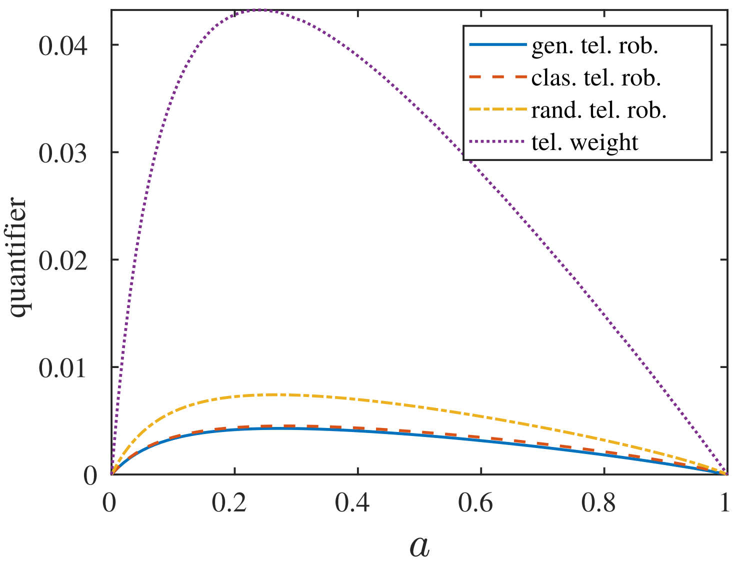

Figure 7.5: Dependence of the teleportation quantifiers introduced here on parameter a a the Horodecki state, using a tomographically complete set of input states (chosen randomly to produce this plot), and a partial Bell State Measurement. For all values of $a \neq$ 0 or 1, non-classical teleportation is demonstrated. Separability of the channel operators was relaxed to the requirement of having a 2-symmetric PPT extension [DPS02].

give higher weights, even maintaining a partial Bell state measurement. For example, the "pyramid" unextendable product bases (UPB) state [Ben+99], with tomographically complete set of inputs, has teleportation weight equal to 0.2350.

7.3.4 Estimating entanglement negativity from a teleportation experiment

As shown in the previous sections, different types of teleportation robustness can put a lower bound on the corresponding types of entanglement robustness. The naturally arising question is whether teleportation experiments can provide lower bounds to some other entanglement quantifiers. Negativity of entanglement [VW02] is a widely used entanglement measure, which is largely due to the fact that it can be computed efficiently. Already in the original paper introducing the entanglement negativity [VW02] the authors found that for some states it puts a lower bound on its teleportation capacity. Here we will prove that by using all the accessible information from a teleportation experiment one can put a lower bound on the entanglement negativity of the shared state ρ^{AB}.

As explained in Sec. 2.1.2 the entanglement negativity of a state ρ^{AB} can be found on the following way:

$$\begin{aligned} \mathscr{N}(\rho^{\mathrm{AB}}) &= \min_{\rho_+,\rho_-} \quad \mathrm{tr}(\rho_-) \\ &\quad \text{s.t.} \qquad \rho^{\mathrm{AB}} = \rho_+ - \rho_- \\ &\qquad\qquad\quad \rho_\pm{}^{T_{\mathrm{A}}} \geq 0. \end{aligned} \tag{7.51}$$

A complete information accessible in a teleportation experiment i.e. knowledge of the teleportation assemblage $\{\sigma_{a|\omega_x}\}_{a,x}$ allows one to construct a semidefinite program whose solution represents a lower bound on the negativity of the shared state ρ^{AB}:

$$\begin{aligned} \min_{\sigma^{\pm}_{a|\omega_x}} \qquad & \sum_a \mathrm{tr}\left(\sigma^-_{a|\omega_x}\right) & (7.52) \\ \text{s.t.} \qquad & \sigma_{a|\omega_x} = \sigma^+_{a|\omega_x} - \sigma^-_{a|\omega_x} \\ & \sigma^{\pm}_{a|\omega_x} = \mathrm{tr}_{\mathrm{V}}\left[M_a^{*\mathrm{VB}}\left(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}}\right)\right] \\ & M_a^{*\mathrm{VB}} \geq 0. & (7.53) \end{aligned}$$

The second line is the equivalent of the constraint $\rho^{\mathrm{AB}} = \rho_+ - \rho_-$ from eq. (7.51), so that

$$\sigma^{\pm}_{a|\omega_x} = \mathrm{tr}_{\mathrm{VA}}\left[\left(M_a^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}} \otimes \rho_{\pm}^{\mathrm{AB}}\right)\right]$$

With this in mind the objective function is easily identified as

$$\sum_a \mathrm{tr}\left(\sigma^-_{a|\omega_x}\right) = \mathrm{tr}\left(\omega_x^{\mathrm{V}} \otimes \rho_-^{\mathrm{AB}}\right) = \mathrm{tr}\left(\rho_-^{\mathrm{AB}}\right) \tag{7.54}$$

The last constraint characterizes the effective measurements coming from a PPT state. From eq. (7.25) we get

$$d\left(M_a^{*\mathrm{VB}}\right)^T = \mathrm{tr}_{\mathrm{V_1A}}\left[\left(\mathbb{1}^{\mathrm{V}} \otimes M_a^{\mathrm{V_1A}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\Phi_+^{\mathrm{VV_1}} \otimes \rho^{\mathrm{AB}\,T_{\mathrm{B}}}\right)\right]. \tag{7.55}$$

If the state ρ^{AB} is PPT the l.h.s. of the last equation represents an unnormalized quantum state which means that operators $\left(M_a^{*\mathrm{VB}}\right)^T$ and hence $\left(M_a^{*\mathrm{VB}}\right)$ are also positive, which justifies the last constraint from Eq. (7.52).

Now we need to prove that the solution to (7.52) lower bounds the negativity of entanglement of the state ρ^{AB} given as the solution of (7.51). First let us note that in the case the set of input states is tomographically complete and Alice applies the Bell state measurement the solutions to (7.51) and (7.52) coincide. To see that, let us rewrite the optimization problem (7.52) for $a = 0$ given that $M_0^{\mathrm{VA}} = \Phi_+^{\mathrm{VA}}$:

$$\begin{aligned}
\min_{\rho_\pm} \quad & \mathrm{tr}\rho_- && (7.56)\\
\text{s.t.} \quad & \mathrm{tr}_{\mathrm{VA}}\left[\left(\Phi_+^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}} \otimes \rho^{\mathrm{AB}}\right)\right] = \mathrm{tr}_{\mathrm{VA}}\left[\left(\Phi_+^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}} \otimes \left(\rho_+^{\mathrm{AB}} - \rho_-^{\mathrm{AB}}\right)\right)\right] \\
& \sigma^{\pm}_{a|\omega_x} = \mathrm{tr}_{\mathrm{V}}\left[{M^*_{a,\pm}}^{\mathrm{VB}}\left(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}}\right)\right] \\
& M_a^{*\mathrm{VB}} = \mathrm{tr}_{\mathrm{A}}\left[\left(M_{a,\pm}^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\mathbb{1}^{\mathrm{V}} \otimes \rho_\pm^{\mathrm{AB}}\right)\right] = \frac{1}{d}\rho_\pm^{T_{\mathrm{B}}} \geq 0.
\end{aligned}$$

The first constraint in case of a tomographically complete set of inputs is satisfied if and only if

$$\rho_{\mathrm{AB}} = \rho_+ - \rho_-,$$

which finally reduces (7.52) to (7.51). For the other values of a the constraints from (7.56) are authomatically satisfied. The first constraint can be rewritten as

$$\begin{aligned}
&\mathrm{tr}_{\mathrm{VA}}\left[\left(U_a^{\mathrm{V}}\Phi_+^{\mathrm{VA}}{U_a^\dagger}^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}} \otimes \rho^{\mathrm{AB}}\right)\right] = \\
&= \mathrm{tr}_{\mathrm{VA}}\left[\left(U_a^{\mathrm{V}}\Phi_+^{\mathrm{VA}}{U_a^\dagger}^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left(\omega_x^{\mathrm{V}} \otimes \left(\rho_+^{\mathrm{AB}} - \rho_-^{\mathrm{AB}}\right)\right)\right]
\end{aligned}$$

which is equivalent to

$$\begin{aligned}
&\mathrm{tr}_{\mathrm{VA}}\left[\left(\Phi_+^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left({U_a^\dagger}^{\mathrm{V}}\omega_x^{\mathrm{V}}U_a^{\mathrm{V}} \otimes \rho^{\mathrm{AB}}\right)\right] = \\
&= \mathrm{tr}_{\mathrm{VA}}\left[\left(\Phi_+^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}}\right)\left({U_a^\dagger}^{\mathrm{V}}\omega_x^{\mathrm{V}}U_a^{\mathrm{V}} \otimes \left(\rho_+^{\mathrm{AB}} - \rho_-^{\mathrm{AB}}\right)\right)\right].
\end{aligned}$$

If the set $\{\omega_x\}_x$ is tomographically complete so is $\{U_a^\dagger \psi_x U_a\}_x$, and thus the last statement is equivalent to $\rho_{\mathrm{AB}} = \rho_+ - \rho_-$. Similarly the last constraint from (7.56) reduces to $U_a\rho_\pm^{T_{\mathrm{B}}}U_a^\dagger \geq 0$, which is satisfied if $\rho_\pm^{T_{\mathrm{B}}} \geq 0$. Thus, we see that when Alice applies the full Bell state measurement and has access to a tomographically complete set of input states, the optimization problems (7.52) and (7.51) are equivalent.

In a general case, note that the states $\rho'_\pm$ leading to the optimal solution of (7.51) by forming $\sigma^{\pm}_{a|\omega_x} = \mathrm{tr}_{\mathrm{VA}}[(M_a^{\mathrm{VA}} \otimes \mathbb{1}^{\mathrm{B}})(\omega_x^{\mathrm{V}} \otimes \rho_\pm^{\mathrm{AB}})]$ with arbitrary measurements $\{M_a^{\mathrm{VA}}\}$ and input states $\{\omega_x\}_x$ satisfy all the constraints of (7.52). The equivalence between the objective functions follows from Eq. (7.54) and the last constraint is satisfied due to (7.55). This means that the solution to (7.52) cannot be higher than $\mathcal{N}(\rho^{\mathrm{AB}})$, i.e. it puts a lower bound to the entanglement negativity of ρ^{AB}.

7.4 Teleportation witnesses

An advantage of having an SDP formulation for certifying the non-classicality of teleportation is that it also provides linear constraints satisfied by any teleportation data that admits a classical scheme, which generalize the average fidelity of teleportation. These constraints work as *non-classical teleportation witnesses*, which, similarly to the idea entanglement witnesses, can be used to test the non-classicality of any experimental teleportation data. Let us consider a slightly different form of the SDP (7.21) for finding the random teleportation robustness

$$\begin{aligned}
\text{given} \quad & \{\sigma_{a|\omega_x}\}_{a,x}, \\
\min_{\{M_a^{*\,\mathrm{VB}}\}} \quad & r \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (7.57)\\
\text{s.t.} \quad & \sigma^{\mathrm{B}}_{a|\omega_x} + r\frac{\mathbb{1}^{\mathrm{B}}}{o_{\mathrm{A}}d} = \mathrm{tr}_{\mathrm{V}}[M_a^{*\,\mathrm{VB}}(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}})] \quad \forall a,x, \\
& \sum_a M_a^{*\,\mathrm{VB}} = \mathbb{1}^{\mathrm{V}} \otimes (\rho^{\mathrm{B}} + r\frac{\mathbb{1}^{\mathrm{B}}}{d}) \\
& M_a^{*\,\mathrm{VB}} \in \Sigma \quad \forall a, \\
& r \geq 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (7.58)
\end{aligned}$$

It differs from (7.21) in fixing $p(a) = 1/o_{\mathrm{A}}$, omitting the common denominator $(1+r)$ and adding the trivial constraint $r \geq 0$.
The Lagrangian for (7.57) is

$$\begin{aligned}
\mathscr{L} = r &+ \mathrm{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x}\left(\sigma^{\mathrm{B}}_{a|\omega_x} + r\frac{\mathbb{1}^{\mathrm{B}}}{o_{\mathrm{A}}d} - \mathrm{tr}_{\mathrm{V}}[M_a^{*\,\mathrm{VB}}(\omega_x^{\mathrm{V}} \otimes \mathbb{1}^{\mathrm{B}})]\right) + \\
&+ \mathrm{tr}\, G^{\mathrm{VB}}\left(\sum_a M_a^{*\,\mathrm{VB}} - \mathbb{1}^{\mathrm{V}} \otimes (\rho^{\mathrm{B}} + r\frac{\mathbb{1}^{\mathrm{B}}}{d})\right) - \mathrm{tr}\sum_a H_a^{\mathrm{VB}} M_a^{*\,\mathrm{VB}} - \mu r, \\
&= r\left(1 + \frac{1}{o_{\mathrm{A}}d}\mathrm{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x} - \frac{1}{d}\mathrm{tr}\, G^{\mathrm{VB}} - \mu\right) + \mathrm{tr}\sum_a M_a^{*\,\mathrm{VB}}\left(-\sum_x \omega_x^{\mathrm{B}} \otimes F^{\mathrm{B}}_{a|\omega_x} + G^{\mathrm{VB}} - H_a^{\mathrm{VB}}\right) \\
&\quad + \mathrm{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x}\sigma^{\mathrm{B}}_{a|\omega_x} - \mathrm{tr}[G^{\mathrm{B}}\rho^{\mathrm{B}}] \qquad\qquad (7.59)
\end{aligned}$$

where $\{F^{\mathrm{B}}_{a|\omega_x}\}_{a,x}$, G^{VB}, $\{H_a^{\mathrm{VB}}\}_a$, and μ are the Lagrange multipliers corresponding to each set of constraints respectively. By taking $H_a^{\mathrm{VB}} \in \mathscr{W}$, where $\mathscr{W} = \{W|\,\mathrm{tr}[W\rho^{\mathrm{sep}}] \geq 0, \forall\rho^{\mathrm{sep}} \in \Sigma\}$ is the set of entanglement witnesses (operators which are positive on all separable operators), and $\mu \geq 0$, then by enforcing that the first and second brackets vanish, we can ensure $\mathscr{L} \leq r$ and thus the dual formulation of (7.57) is

$$\begin{aligned}
\text{given} \quad & \{\sigma^{\mathrm{B}}_{a|\omega_x}\}_{a,x}, \\
\max_{\{F_{a|\omega_x}^{\mathrm{B}}\}, G^{\mathrm{VB}}, \{H_a^{\mathrm{VB}}\}} \quad & \operatorname{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x}\sigma^{\mathrm{B}}_{a|\omega_x} - \operatorname{tr}[G^{\mathrm{B}}\rho^{\mathrm{B}}] \\
\text{s.t.} \quad & 1 + \frac{1}{o_{\mathrm{A}}d}\operatorname{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x} - \frac{1}{d}\operatorname{tr}G^{\mathrm{VB}} - \mu = 0, \\
& -\sum_x \omega_x^{\mathrm{V}} \otimes F^{\mathrm{B}}_{a|\omega_x} + G^{\mathrm{VB}} - H_a^{\mathrm{VB}} = 0 \quad \forall a, \\
& H_a^{\mathrm{VB}} \in \mathscr{W} \quad \forall a, \\
& \mu \geq 0.
\end{aligned} \tag{7.60}$$

It is seen that $\{H_a^{\mathrm{VB}}\}_a$ and μ play the role of slack variables (they do not appear in the objective function), and can thus be eliminated from the problem, to arrive at the equivalent formulation

$$\begin{aligned}
\text{given} \quad & \{\sigma^{\mathrm{B}}_{a|\omega_x}\}_{a,x}, \\
\max_{\{F_{a|\omega_x}^{\mathrm{B}}\}, G^{\mathrm{VB}}} \quad & \operatorname{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x}\sigma^{\mathrm{B}}_{a|\omega_x} - \operatorname{tr}[G^{\mathrm{B}}\rho^{\mathrm{B}}] \\
\text{s.t.} \quad & 1 + \frac{1}{o_{\mathrm{A}}d}\operatorname{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x} - \frac{1}{d}\operatorname{tr}G^{\mathrm{VB}} \geq 0, \\
& -\sum_x \omega_x^{\mathrm{V}} \otimes F^{\mathrm{B}}_{a|\omega_x} + G^{\mathrm{VB}} \in \mathscr{W} \quad \forall a,
\end{aligned} \tag{7.61}$$

By taking all dual variables to be proportional to the identity, it is straightforward to see that all constraints can be strictly satisfied, and hence strong duality holds. As such, the optimal value of the primal and dual formulations coincide.

7.4.1 Examples

Consider the teleportation of the states $\{\omega_x\}_x = \{|0\rangle, |1\rangle, (|0\rangle \pm |1\rangle)/\sqrt{2}, (|0\rangle \pm i|1\rangle)/\sqrt{2}\}$ using the two-qubit Werner state

$$\rho^{\mathrm{AB}} = p|\Phi^+\rangle\langle\Phi^+| + (1-p)\frac{\mathbb{1}^{\mathrm{AB}}}{4} \tag{7.62}$$

and full Bell state measurement, $\{M_a^{\mathrm{VA}}\}_a = \{|\Phi^+\rangle\langle\Phi^+|, |\Psi^+\rangle\langle\Psi^+|, |\Phi^-\rangle\langle\Phi^-|, |\Psi^-\rangle\langle\Psi^-|\}$. The teleportation witness is given in Table 7.1 [2]. We have $\operatorname{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x}\sigma^{B}_{a|\omega_x} = 6(\frac{1}{3} - p)$,

[2] In this section we denote Pauli matrices with X,Y and Z, unlike the previous sections where they were denoted with σ_{X},σ_{Y} and σ_{Z}. This is to avoid confusion between Pauli operators and teleportation assemblage elements $\sigma_{a|\omega_x}$.

and therefore teleportation is certified for all $p > 1/3$, which coincides with the separability bound of the state (7.62). Finally, we note that

$$\{W_a\}_a = \{4|\Psi^-\rangle\langle\Psi^-|, 4|\Phi^-\rangle\langle\Phi^-|, 4|\Psi^+\rangle\langle\Psi^+|, 4|\Phi^+\rangle\langle\Phi^+|\} \tag{7.63}$$

and thus $\mathrm{tr}[W_a\rho_{\mathrm{sep}}] \geq 0$ as required by (7.61).

		x					
	$F^{\mathrm{B}}_{a\vert\omega_x}$	0	1	2	3	4	5
	0	$\frac{\mathbb{1}}{3}-X$	$\frac{\mathbb{1}}{3}+X$	$\frac{\mathbb{1}}{3}-Y$	$\frac{\mathbb{1}}{3}+Y$	$\frac{\mathbb{1}}{3}-Z$	$\frac{\mathbb{1}}{3}+Z$
a	1	$\frac{\mathbb{1}}{3}-X$	$\frac{\mathbb{1}}{3}+X$	$\frac{\mathbb{1}}{3}+Y$	$\frac{\mathbb{1}}{3}-Y$	$\frac{\mathbb{1}}{3}+Z$	$\frac{\mathbb{1}}{3}-Z$
	2	$\frac{\mathbb{1}}{3}+X$	$\frac{\mathbb{1}}{3}-X$	$\frac{\mathbb{1}}{3}+Y$	$\frac{\mathbb{1}}{3}-Y$	$\frac{\mathbb{1}}{3}-Z$	$\frac{\mathbb{1}}{3}+Z$
	3	$\frac{\mathbb{1}}{3}+X$	$\frac{\mathbb{1}}{3}-X$	$\frac{\mathbb{1}}{3}-Y$	$\frac{\mathbb{1}}{3}+Y$	$\frac{\mathbb{1}}{3}+Z$	$\frac{\mathbb{1}}{3}-Z$

Table 7.1: Teleportation witness for the two-qubit Werner state (7.62). The verifier provides the states $\{\omega_x\}_x = \{|0\rangle, |1\rangle, (|0\rangle \pm |1\rangle)/\sqrt{2}, (|0\rangle \pm i|1\rangle)/\sqrt{2}\}$ to Alice. By measuring the observables $F^{\mathrm{B}}_{a|\omega_x}$ when Bob forwards the state $\sigma^{\mathrm{B}}_{a|\omega_x}$ to the verifier, the value $\mathrm{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x}\sigma^{B}_{a|\omega_x} = 6(\frac{1}{3} - p)$ is obtained, which is negative for all $p > 1/3$. Thus all entangled two-qubit Werner states are witnessed as useful for teleportation.

Consider now the so-called 'tiles' bound entangled state [Ben+99]:

$$\rho_{\mathrm{tiles}} = \frac{1}{4}\left(\mathbb{1} - \sum_{i=0}^{4} |\phi_i\rangle\langle\phi_i|\right), \tag{7.64}$$

where the states $|\phi_i\rangle$ form a UPB:

$$\begin{aligned} |\phi_0\rangle &= \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle), & |\phi_1\rangle &= \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle), \\ |\phi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle, & |\phi_3\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle, \end{aligned} \tag{7.65}$$

$$|\phi_4\rangle = \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle).$$

According to the benchmark based on the average fidelity this state is useless for teleportation [HHH99]. For the set of input states $\{\omega_x\}_x = \{|0\rangle, |2\rangle, (|0\rangle - |1\rangle)/\sqrt{2}, (|1\rangle - |2\rangle)/\sqrt{2}, (|0\rangle + |1\rangle + |2\rangle)/\sqrt{3}, \mathbb{1}/3\}$ and partial Bell state measurement which projects on $|\Phi^+\rangle\langle\Phi^+|$, we generate the teleportation witness given in Table 7.2. The state achieves the value $\mathrm{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x}\sigma^{\mathrm{B}}_{a|\omega_x} = -\varepsilon/3$, which shows that the bound entangled states are in fact useful for teleportation.

A couple of additional comments are in order. First, note that the set of input states $\{\omega_x\}_x$ in this instance is not even tomographically complete, and yet teleportation can

		x					
	$F^{\mathrm{B}}_{a\vert\omega_x}$	0	1	2	3	4	5
a	0	ω_2	ω_3	ω_1	ω_0	ω_4	$-3\varepsilon\mathbb{1}$
	1	0	0	0	0	0	0

Table 7.2: Teleportation witness for the two-qutrit bound entangled 'tiles' state (7.64). The verifier provides the states $\{\omega_x\}_x = \{|0\rangle\langle 0|, |2\rangle\langle 2|, (|0\rangle - |1\rangle)(\langle 0| - \langle 1|)/2, (|1\rangle - |2\rangle)(\langle 1| - \langle 2|)/2, (|0\rangle + |1\rangle + |2\rangle)(\langle 0| + \langle 1| + \langle 2|)/3, \mathbb{1}/3\}$ to Alice. Here, $\varepsilon \in (0, 0.02842]$. By measuring the observables $F^{\mathrm{B}}_{a|\omega_x}$ when Bob forwards the state $\sigma^{\mathrm{B}}_{a|\omega_x}$ to the verifier, the value $\mathrm{tr}\sum_{a,x} F^{\mathrm{B}}_{a|\omega_x} \sigma^{B}_{a|\omega_x} = -\varepsilon/3$ is obtained. This demonstrates the fact that, contrary to what is usually claimed, bound entangled states are useful for teleportation.

nevertheless be certified. Second, here we considered only a partial Bell state measurement. Since M^{VA}_1 is a separable operator in this instance, it is for this reason that $F^{\mathrm{B}}_{1|\omega_x}$ vanish. Finally, we note that $W_0 = \sum_x \omega^{\mathrm{V}}_x \otimes F^{\mathrm{B}}_{1|\omega_x} = \sum_i |\phi_i\rangle\langle\phi_i| - \varepsilon\mathbb{1}$ is precisely the entanglement witness which is violated by the 'tiles' UPB state (7.64) for $\varepsilon \in (0, 0.02842]$ [Güh+02]. This demonstrates that the constraint in (7.61) is indeed satisfied.

7.5 Teleportation as a type of nonlocality

The results presented so far in this chapter indicate that it is highly beneficial to regard teleportation as a specific nonlocality scenario. In this section we compare teleportation to the other known types of nonlocality and discuss these relations in more details. To facilitate the discussion let us recapitulate the main properties of Bell nonlocality and EPR-steering, before continuing with the other modifications of the standard Bell scenario.

We start with the concept of Bell nonlocality (for more details see Sec. 2.2), describing the correlations between Alice's and Bob's measurement outcomes. All experimental devices are treated as black boxes, corresponding to the so-called device-independent scenario [Aci+07, CK11]. The parties choose the measurements by sending classical inputs to their black boxes. All conclusions about the systems are drown solely from the set of the conditional correlations probabilities $\{p(a,b|x,y)\}$, obtained by the Born rule

$$p(a,b|x,y) = \mathrm{Tr}\left[\left(M^{\mathrm{A}}_{a|x} \otimes M^{\mathrm{B}}_{b|y}\right)\rho^{\mathrm{AB}}\right]$$

where $M_{a|x}$ and $M_{b|y}$ are Alice's and Bob's measurements respectively and ρ^{AB} is the shared state. If the probability distribution $\{p(a,b|x,y)\}$ is nonlocal it excludes the existence of the local hidden variable models for the outputs of Alice's and Bob's measurements [Bell64].

Different relaxations of the device-independent scenario lead to different types of nonlocality (See Fig. 7.7). Another fundamentally and practically important type of nonlocality is EPR-steering [WJD07, CS17] (for more details see Section 2.4). It differs from Bell nonlocality in the fact that Bob's measurements are fully characterized. In particular, it can be assumed that Bob is able to perform full state tomography on his system. Thus, EPR-steering describes correlations between Alice's measurement outputs and the states prepared for Bob. Bob's reduced states following Alice's different measurement have the following form

$$\sigma_{a|x} = \mathrm{Tr}_{\mathrm{A}}\left[\left(M^{\mathrm{A}}_{a|x} \otimes \mathbb{1}^{\mathrm{B}}\right)\rho^{\mathrm{AB}}\right].$$

The set $\{\sigma_{a|x}\}_{a,x}$ is termed assemblage and it is said to be steerable if there is no local hidden state model for the outputs of Alice's measurements and corresponding Bob's states. The scenario native to EPR steering is termed one-sided-device-independent and it has proven to be useful for various quantum information protocols [PCPA15, LTBS14, ŠH16, GWK17].

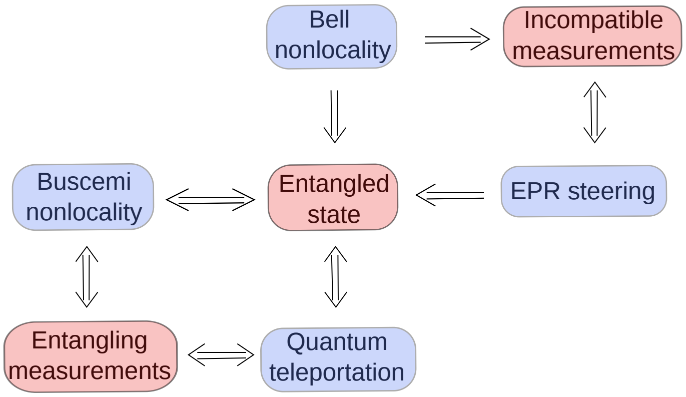

Figure 7.6: The relations among different types of nonlocality (blue boxes) and necessary resources(red boxes). Presence of any of the four types of nonlocality implies the presence of entanglement in the underlying system. While some entangled states never lead to Bell nonlocality or steering, every entangled state can lead to Buscemi nonlocality and quantum teleportation. The resource for EPR steering and Bell nonlocality are incompatible measurements. Every set of incompatible measurements can demonstrate EPR steering, while some sets of incompatible measurement cannot demonstrate to Bell nonlocality. The necessary resource for Buscemi nonlocality and quantum teleportation are entangling joint measurements. Every entangling measurement can demonstrate both Buscemi nonlocality and quantum teleportation.

Another relaxation of the device-independent scenario is obtained when Alice and

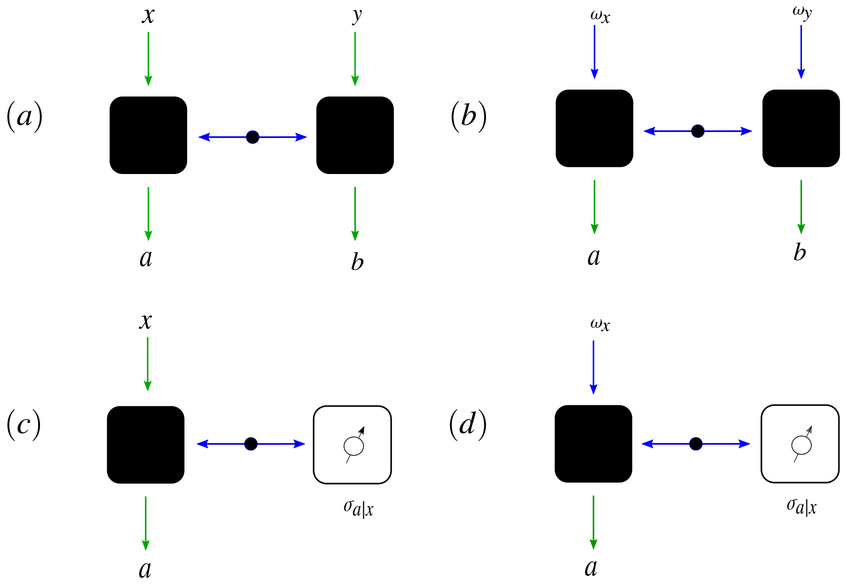

Figure 7.7: Scenario (a) corresponds to Bell nonlocality, (b) represents Buscemi nonlocality, (c) EPR steering and (d) quantum teleportation. The transition from left to right corresponds to the exchange of classical inputs with quantum ones, while the transition from top to bottom corresponds to characterising measurement devices of one of the parties.

Bob use quantum states as inputs, while the boxes still return classical outputs. This scenario, known as measurement-device-independent [BRLG13], was introduced by Buscemi [Bus12] leading to the new type of nonlocality, here termed Buscemi nonlocality (for more details check Section 6.1). All measurement devices and the source of the shared state are treated as black boxes but both Alice and Bob have a trusted preparation device. The only source of information about the system are the correlation probabilities

$$p(a,b|\omega_x,\omega_y) = \left[\left(M_a^{\mathrm{A'A}} \otimes M_b^{\mathrm{BB'}}\right)\left(\omega_x^{\mathrm{A'}} \otimes \rho^{\mathrm{AB}} \otimes \omega_y^{\mathrm{B'}}\right)\right]$$

which are obtained when Alice and Bob apply joint measurements M_a and M_b on their part of the shared state ρ^{AB} and the quantum inputs ω_x and ω_y respectively. The remarkable fact about measurement-device-independent scenario is that every entangled state can lead to Buscemi nonlocal correlation probabilities.

Finally, quantum teleportation is positioned in the intersection of the two above mentioned relaxations of the device-independent scenario. In, what would be called, one-sided measurement-device-independent scenario Alice uses quantum states as inputs for her black box, while Bob can apply quantum state tomography to his share of the state. This scenario exactly describes what is happening in a quantum teleportation experiment.

Putting teleportation in this context enables applying the well developed framework for exploring different forms of nonlocality to teleportation experiments. Rephrasing it in the language of nonlocality, quantum teleportation manifests in the nonlocal correlation between Alice's joint measurement outputs and states prepared for Bob. The states to be teleported are just the quantum inputs for Alice's box, while teleported states correspond to reduced states of Bob forming a kind of *teleportation assemblage* (teleportage in [HS17]). Consequently, a teleportation experiment is non-classical if it excludes a ”local hidden channel model”, which would in a classical way correlate Alice's outputs with Bob's reduced states (like, for example, in the model described in [PM95]).

7.6 Discussion

In this Chapter we have studied quantum teleportation using the full data available in an experiment. We have shown that this allows us to test directly whether the data has any classical explanation via the method of semidefinite programming. Using the full data, every entangled state can be certified to implement non-classical teleportation, and we show that this can be tested in an experimentally friendly way using a teleportation witness. This overthrows the popular belief that not all entangled states are useful for teleportation (in particular bound entangled states), a conclusion which was based upon a single figure of merit, the average fidelity of teleportation, which our teleportation witnesses generalize. We introduced several teleportation quantifiers which allow us to compare compatible teleportation experiments. Moreover, each introduced teleportation quantifier can be used to bound the amount of entanglement the parties are sharing.

In the future research it would be interesting to see which properties of teleportation can be mirrored in some other important protocols such as remote state preparation or quantum secret sharing. Also, it may be instructive to see if these new insights in the relation between entanglement and teleportation affect some more complex quantum information protocols which use teleportation as a sub-routine.

Chapter 8

Universal device-independent entanglement certification

Any protocol for entanglement detection has to deal with a trade-off between the generality, *i.e.* the degree of applicability and the amount of required resources. On one side is certification of entanglement through entanglement witnesses, as described in Section 2.1.1. This approach is fully general, meaning that every entangled state can be certified in this way, but it requires the precise characterisation of the measurements performed in the process. Failing to account for all the errors and deviations in the experimental set-up leads to either a false certification or loss of the universality of the approach [Ros+12]. On the other side lies device-independent entanglement certification, exploiting nonlocal correlations stemming from entangled states which violate a Bell inequality. This approach makes minimal assumptions about the experimental set-up, treating all devices as black boxes, but fails when it comes to the universality. As described in the introductory remarks of Chapter 6, there are entangled states which never produce nonlocal correlations.

Various semi-device-independent approaches represent the middle ground between entanglement witnesses and DI entanglement certification. In principle, the more relaxed device-independence of the approach is, the more entangled states can be certified. In section 6.1 we discussed *measurement-device-independent entanglement witnessing* (MDIEW), introduced in [Bus12]. This approach can be used to certify all entangled states, but it is not fully device-independent because the set-up involves a trusted preparation device. It is used to prepare states which serve as quantum inputs to the black boxes.

In this chapter we construct a fully device-independent protocol for certification of all entangled states. It combines results from the field of self-testing with ideas from MDIEW. The lack of characterized preparation device necessary for MDIEW is compensated by moving to the quantum network set-up. Intuitively, our protocol can be understood as a device-independent extension of MDIEWs, in which the input quantum states are certified device-independently through a self-testing protocol.

8.1 Protocol for device-independent certification of all entangled states

In this section we define the set-up for the device independent certification of entanglement in bipartite systems and give an informal description of the protocol. The generalization to the multipartite states is straightforward and will be discussed in the conclusion of this chapter. As outlined in the introductory remarks, the entanglement of a bipartite state ρ^{AB} is certified by putting the state in a quantum network. Two parties holding the shares of the state ρ^{AB} are named Alice and Bob. The set-up involves two additional parties, Charlie and Daisy. Charlie and Alice share state ρ^{CA_0}, Bob and Daisy $\rho^{\mathrm{B}_0\mathrm{D}}$, and as stated before, Alice and Bob share the state ρ^{AB}. Hence, Alice and Bob, each have two systems in their boxes labelled by A_0 and A for Alice and B_0 and B for Bob. All parties treat their devices as black boxes, exchanging classical messages with them. Classical inputs sent to the boxes are denoted by x for Alice, y for Bob, z for Charlie and w for Daisy, and corresponding outputs, returned by boxes, are denoted by a for Alice, b for Bob, c for Charlie and d for Daisy. Inputs label the choice of measurement, while the outputs represent the obtained outputs. For example, a pair (x,a) corresponds to applying a POVM $M_{a|x}$, and similarly for the other parties. At the end, the protocol is characterized by the joint conditional probability distributions $p(a,b,c,d|z,x,y,w)$.

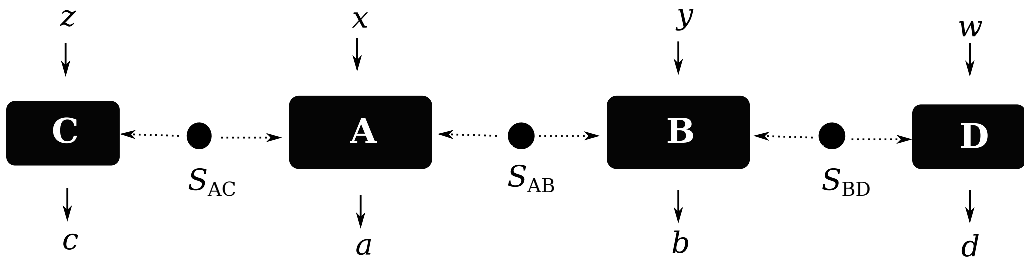

Figure 8.1: The scenario for the fully device-independent certification of all entangled states. Four parties are involved sharing the states emitted from three independent sources. The source S_{AB} emits the state ρ^{CA_0}, shared by Charlie and Alice. The source S_{AB} emits the state ρ^{AB} shared by Alice and Bob. Finally, the source S_{BD} emits the state $\rho^{\mathrm{B}_0\mathrm{D}}$. In the ideal specification, the state ρ^{AB} is entangled while the states ρ^{CA_0} and $\rho^{\mathrm{B}_0\mathrm{D}}$ are maximally entangled.

Let us recall that Alice and Bob can certify every entangled state if both have access to a tomographically complete set of quantum states, which they treat as inputs for the black boxes (for more details see Ch. 6, Sec. 6.1). This scenario allows for the aforementioned MDI entanglement certification protocol. Observe that the protocol can be modified by exchanging the preparation device with a form of the remote state preparation in the scenario from Fig. 8.1. Assume that each of the two auxiliary states ρ^{CA_0} and $\rho^{\mathrm{B}_0\mathrm{D}}$ is a maximally entangled state $|\Phi^+\rangle$. In that case Charlie and Daisy can steer Alice's and Bob's states by applying the corresponding projective measurements. Assume that $\rho^{\mathrm{CA}_0} = |\Phi^+\rangle\langle\Phi^+|$ and $M_{c|z} = |0\rangle\langle 0|$. Then, upon Charlie's measurement Alice's system is in the state

$$\mathrm{tr}_{\mathrm{C}}\left[(|0\rangle\langle 0|^{\mathrm{C}} \otimes \mathbb{1}^{\mathrm{A}_0})|\Phi^+\rangle\langle\Phi^+|^{\mathrm{CA}_0}\right] \sim |0\rangle\langle 0|^{\mathrm{A}_0}.$$

In a similar manner Charlie can remotely prepare for Alice other states from a tomographically complete set of input states Ψ. Analogously, Daisy can steer Bob's system B_0 to any element from the same set Ψ. Alice and Bob can use the states from the set Ψ as quantum inputs and continue performing entanglement certification task in the same way as they would perform a MDIEW. The advantage of the protocol based on the remote preparation compared to the standard MDIEW is that former can be formulated in a device-independent manner. For that purpose we used the self-testing techniques. Indeed, self-testing protocols can be used to certify in a device-independent way that the state ρ^{CA_0} ($\rho^{\mathrm{B}_0\mathrm{D}}$) is equivalent to the maximally entangled state $|\Phi^+\rangle$ and that measurements $\{M_{z|c}\}_{z,c}$ ($\{M_{d|w}\}_{d,w}$) are indeed those necessary to prepare the states Alice (Bob) needs. For the certification of entanglement in qubit states the simple modification of known self-testing protocols ([MY04, MYS14, Kan16]) will suffice. For states of a generic local dimension, the adaptation of the existing self-testing protocols to the form useful for entanglement certification will require a more careful approach. This will be the main topic of Section 8.2.

Here we will outline the protocol for fully device-independent entanglement certification of all entangled states:

1. *Self-testing part.* Partial conditional probability distributions $p(c,a|z,x)$ and $p(b,d|y,w)$ are collected and used to certify that Alice with Charlie and Bob with Daisy shares a maximally entangled pair of qudits.

2. *Entanglement witnessing.* Full conditional probability distributions $p(c,a,b,d|z,x,y,w)$ are used to certify the entanglement of ρ^{AB} by using the analogue of MDIEW introduced in Chapter 6.

8.2 Self-testing maximally entangled states and Pauli observables

In this section we describe the self-testing of the maximally entangled states and an informationally complete set of measurements. As outlined in the previous section Alice

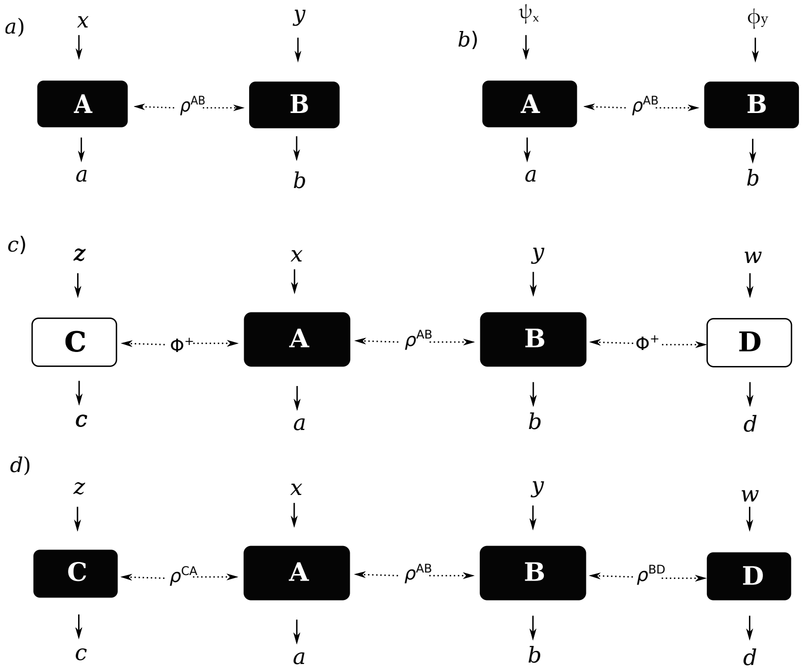

Figure 8.2: (a) Standard Bell scenario for device independent entanglement certification. The estimated probabilities $p(ab|xy)$ are tested for violation of a Bell inequality in order to certify the entanglement of the state ρ_{AB}. (b) Scenario for MDI entanglement certification. Here, the inputs are given by trusted quantum states ψ_x and ϕ_y. (c) Equivalent MDI scenario in which the inputting of the states ψ_x and ϕ_y in scenario (b) is replaced by giving Alice and Bob each one half of a maximally entangled state and performing local measurements on them. (d) Our proposal for DI entanglement certification. The entangled state ρ^{AB} to be detected is placed in a network containing additional auxiliary entangled states. Using self-testing techniques, these entangled states are certified to be maximally entangled and perform the expected measurements as required in (c).

has to perform such a self-test with Charlie and Bob with Daisy. Since the role of Alice and Charlie is completely equivalent to the role of Bob and Daisy we will concentrate on the former, with all the conclusions holding for the latter pair. The simplified set-up we consider here involves two parties, Charlie and Alice, who share the quantum state $|\psi\rangle^{\text{CA}_0}$ [1] and perform local measurements labelled by z and x, obtaining outcomes c and a. In accordance with the Born rule the partial conditional probabilities can be written as

$$p(ca|zx) = \text{tr}\left[(M^{\text{C}}_{c|z} \otimes M^{\text{A}_0}_{a|x})|\psi\rangle\langle\psi|^{\text{CA}_0}\right], \tag{8.1}$$

[1] To simplify notation in this chapter we depart from the notation used in Part I, where physical states were primed and reference non-primed. Here reference state will always be either $|\Phi^+\rangle$ or a tensor product of $|\Phi^+\rangle$-s

where $M_{c|z}, M_{a|x}$ denote the local projective measurement operators applies by Charlie and Alice respectively. Note that the self-testing scenario allows us to work with purifications $|\psi\rangle^{\mathrm{CA_0}}$ instead of possibly mixed states $\rho^{\mathrm{CA_0}}$, and assume that all applied measurements are projective.

The basics of self-testing were introduced in Ch. 2 Sec. 2.5 and further discussed as the main topic of chapters 3, 4, 5 and **??**. For easier reading, let us reproduce here the most important concepts related to the self-testing of maximally entangled states. The conditional probabuilities $p(ca|xz)$ self-test the reference quantum state reference quantum state $|\Phi^+\rangle = \sum_{i=0}^{d-1} |ii\rangle$, if they are produced uniquely by $|\Phi^+\rangle$ up to a certain equivalence class. The equivalence class is captured by the notion of a local isometry, which takes into account the possibility of all physical transformations which leave the observed probability distributions invariant. Such operations are local unitary operations applied to the state and measurements, possible embedding in a Hilbert space of larger dimension and/or the existence of additional degrees of freedom. Thus, we say that the correlations $p(ca|zx)$ self-test the state $|\Phi^+\rangle \in \mathscr{H}^{\mathrm{C}'} \otimes \mathscr{H}^{\mathrm{A}_0'}$ if for all states and all measurement operators satisfying Eq. (8.1) there exist Hilbert spaces $\mathscr{H}^{\mathrm{C}}$, $\mathscr{H}^{\mathrm{A_0}}$ such that $|\psi\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A_0}}$, a local auxiliary state $|00\rangle \in \mathscr{H}^{\mathrm{C}'} \otimes \mathscr{H}^{\mathrm{A}_0'}$ and a local unitary operator $U = U_{\mathrm{A_0}} \otimes U_{\mathrm{C}}$ such that

$$U\left[|\psi\rangle \otimes |00\rangle\right] = |\mathrm{junk}\rangle \otimes |\Phi^+\rangle\,, \tag{8.2}$$

where $|\mathrm{junk}\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A_0}}$ is any state representing possible uncorrelated additional degrees of freedom. Intuitively, self-testing means proving the existence of local channels (given by the local unitaries and local auxiliary states) which extract the target state $|\Phi^+\rangle$ from the physical state $|\psi\rangle$ into the $\mathscr{H}^{\mathrm{C}'} \otimes \mathscr{H}^{\mathrm{A}_0'}$ space.
Besides self-testing the state $|\Phi^+\rangle$ we are interested in certifying that the measurement operators are equivalent to some target measurements $\{\bar{M}_{c|z}\}$, $\{\bar{M}_{a|x}\}$ acting on $|\Phi^+\rangle$. Self-testing statements are simpler when the target measurements can be expressed using real numbers alone, *i.e.* $(\bar{M}_{c|z})^* = \bar{M}_{c|z}$ for all c,z and $(\bar{M}_{a|x})^* = \bar{M}_{a|x}$ for all a,x. We say that the correlations $p(ca|zx)$ self-test the state $|\Phi^+\rangle$ and real-valued measurements $\{\bar{M}_{c|z}\}$, $\{\bar{M}_{a|x}\}$ if $p(ca|zx)$ self-tests the state $|\Phi^+\rangle$ according to Eq. 8.2 and furthermore

$$U\left[M_{c|z} \otimes M_{a|x}\,|\psi\rangle \otimes |00\rangle\right] = |\mathrm{junk}\rangle \otimes (\bar{M}_{c|z} \otimes \bar{M}_{a|x}\,|\Phi^+\rangle) \tag{8.3}$$

for each c,a,z,x.

The situation is a bit more complicated when the measurements cannot be expressed using real numbers alone, as noted in Section 2.5. This is because observed probability distributions are invariant under complex conjugation of the state and measurement operators:

$$\mathrm{tr}[(\bar{M}_{c|z} \otimes \bar{M}_{a|x})|\Phi^+\rangle\langle\Phi^+|] = \mathrm{tr}[(\bar{M}'^*_{c|z} \otimes \bar{M}^*_{a|x})|\Phi^+\rangle\langle\Phi^+|] \tag{8.4}$$

(where M^* denotes the complex conjugation operation). Note that the complex conjugation is not a physical operation and it is not captured by the concept of a local isometry.

Henceforth, in compliance with the discussion from Section 2.5 and following the method of [McKM11], we introduce additional local Hilbert spaces $\mathscr{H}^{\mathrm{C}''}$ and $\mathscr{H}^{\mathrm{A}''_0}$ which act as a control space for possible complex conjugation of the measurement operators. Our precise definition of self-testing is as follows.

Definition 9.1. *We say that the correlations $p(ca|zx)$ self-test the state $|\Phi^+\rangle \in \mathscr{H}^{\mathrm{C}'} \otimes \mathscr{H}^{\mathrm{A}'_0}$ and (complex-valued) measurements $\{\bar{M}_{c|z}\}$, $\{\bar{M}_{a|x}\}$ if for all states and all measurement operators satisfying* (8.1) *for there exist Hilbert spaces $\mathscr{H}^{\mathrm{C}}$, $\mathscr{H}^{\mathrm{A}_0}$ such that $|\psi\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A}_0}$, a local auxiliary state $|00\rangle \in [\mathscr{H}^{\mathrm{C}''} \otimes \mathscr{H}^{\mathrm{C}'}] \otimes [\mathscr{H}^{\mathrm{A}''_0} \otimes \mathscr{H}^{\rangle'_0}]$ and a local unitary operator $U = U_{\rangle_0} \otimes U_{\mathrm{C}}$ such that*

$$U\left[M_{c|z} \otimes M_{a|x} |\psi\rangle \otimes |00\rangle\right] = \tilde{M}_{c|z} \otimes \tilde{M}_{a|c} [|\mathrm{junk}_0\rangle \otimes |00\rangle + |\mathrm{junk}_1\rangle \otimes |11\rangle] \otimes |\Phi^+\rangle, \quad (8.5)$$

where $|\mathrm{junk}_j\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A}_0}$ are some unknown subnormalized junk states such that $\langle \mathrm{junk}_0|\mathrm{junk}_0\rangle + \langle \mathrm{junk}_1|\mathrm{junk}_1\rangle = 1$ and the $\tilde{M}$ operators are related to the target measurements by

$$\tilde{M}_{c|z} = \mathbb{1}^{\mathrm{C}} \otimes \left[M_0 \otimes \bar{M}_{c|z} + M_1 \otimes (\bar{M}_{c|z})^*\right]; \quad (8.6)$$

$$\tilde{M}_{a|x} = \mathbb{1}^{\mathrm{A}_0} \otimes \left[M_0 \otimes \bar{M}_{a|x} + M_1 \otimes (\bar{M}_{a|x})^*\right], \quad (8.7)$$

with $\mathsf{M}_0 + \mathsf{M}_1 = \mathbb{1}^{\mathrm{C}''}$ and $\langle 0|\mathsf{M}_0|0\rangle = \langle 1|\mathsf{M}_1|1\rangle = 1$.

The measurements given above can be understood as 'controlled conjugation' measurements: one first measures the double primed ancillary systems with the measurement $\{M_0, M_1\}$; conditioned on this outcome, one then measures the target measurement or its complex conjugation on the target state $|\Phi^+\rangle$. The measurement operators and state $|\mathrm{junk}_0\rangle \otimes |00\rangle + |\mathrm{junk}_1\rangle \otimes |11\rangle$ have such form that the potential complex conjugation is correlated between Charlie and Alice, as implied from (8.4). The norm of the vectors $|\mathrm{junk}_j\rangle$ determines the probability for this complex conjugation to happen. In principle this probability is unknown since the self-testing data is not sufficient to infer the norm of these states.

In order to construct the local unitary U used to prove the self-testing statements one typically considers linear combinations of the probabilities $p(c,a|z,x)$ (corresponding to some Bell inequality) of the form

$$\mathscr{I}[p(c,a|z,x)] = \sum_{c,a,z,x} \beta_{c,a,z,x}\, p(c,a|z,x), \quad (8.8)$$

for which the maximal value in quantum theory $\mathscr{I} = \beta_Q$ occurs using the target state and measurements. The observation $\mathscr{I} = \beta_Q$ then implies relations between the state and measurements performed in the experiment via (8.8), and one can prove the existence of the local unitary from the measurement operators themselves.

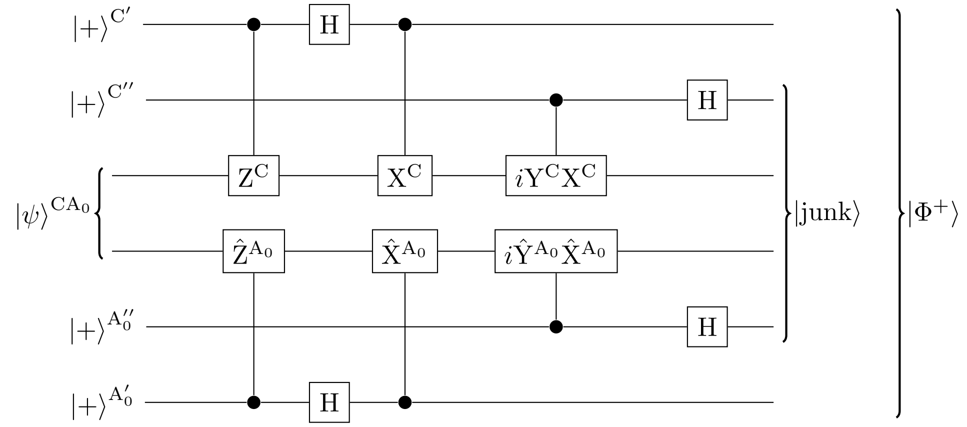

Figure 8.3: Self-testing circuit used for the proof of Lemma 9.5. The unitaries $\hat{Z}^{A_0}$, $\hat{X}^{A_0}$, $\hat{Y}^{A_0}$ can be found in the Appendix A. The target state is extracted into the primed ancillary systems. The double primed ancillary systems are used to control potential complex conjugation of the physical measurements. The circuit is an extension of the partial SWAP gate, first time used in [McKM11].

The majority of the existing self-tests are useful not only for the certification of quantum states but also for the certification of measurements. However, most of them apply to the self-testing of real-valued measurements. The simplest set of measurements which cannot be expressed using real numbers alone is given by the three Pauli observables $\sigma_Z, \sigma_X, \sigma_Y$, acting on maximally entangled pair of qubits. In Section 8.2.1 we prove self-testing statements for these measurements, inspired by the approach of [McKM11] where similar results were obtained. We then extend this to a parallel self-test in sections 8.2.2 and 8.2.3 in order to prove self-testing statements for n-fold tensor products of the Pauli measurements, which form an informationally complete set in dimension 2^n.

8.2.1 Self-testing of Pauli measurements

We begin by proving a self-testing statement for the maximally entangled state of two qubits $|\Phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$ and the three Pauli observables for Charlie. Since there does not exist a basis in which these observables can be written using real numbers only, our self-testing statement will be of the form of Def. 9.1. We note that this is not the first proof of such a result; similar results have been obtained in previous works by generalising the Mayers-Yao self-test [McKM11], by studying the properties of the 'elegant' Bell inequality [APVW16, And+17] and combinations of the CHSH Bell inequality [APVW16] and in a more general approach to the problem [Kan17] focused on commutation relations.

Before proceeding let us clarify the notation. Unless explicitly written, for the sake of shorter expressions, we omit tensor products signs, e.g. $\mathsf{X}^{\mathrm{C}}\left|\psi\right\rangle^{\mathrm{CA}_0}$ should be understood as $\mathsf{X}^{\mathrm{C}}\otimes\mathbb{1}^{\mathrm{A}_0}\left|\psi\right\rangle^{\mathrm{CA}_0}$. This convention then follows for the product of operators, e.g. $\mathsf{X}^{\mathrm{C}}\mathrm{E}_0^{\mathrm{A}}\left|\psi\right\rangle^{\mathrm{CA}_0}$ should be understood as $\mathsf{X}^{\mathrm{C}}\otimes\mathrm{E}_0^{\mathrm{A}}\left|\psi\right\rangle^{\mathrm{CA}_0}$.

The relaxed scenario we consider in this section is as follows. Charlie and Alice share a bipartite quantum state $\left|\psi\right\rangle\in\mathscr{H}^{\mathrm{C}}\otimes\mathscr{H}^{\mathrm{A}_0}$. Charlie has a choice of three measurements $z=1,2,3$, with outcomes $c=\pm1$ denoted by the observables $\mathsf{X}^{\mathrm{C}},\mathsf{Y}^{\mathrm{C}}$ and Z^{C}. Alice has a choice of six ±1 valued measurements $x=1,\cdots,6$, $a=\pm1$, denoted by the observables $\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,z}},\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}},\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,y}},\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,y}},\mathrm{D}^{\mathrm{A}_0}_{\mathrm{y,z}},\mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}}$. Note that each of these observables is Hermitian and unitary. We then consider the following Bell operator (introduced in [APVW16]), which we call the triple CHSH Bell operator

$$\begin{aligned}\mathscr{B}=\mathsf{Z}^{\mathrm{C}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,z}}+\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}})+\mathsf{X}^{\mathrm{C}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,z}}-\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}})+\mathsf{Z}^{\mathrm{C}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{y,z}}+\mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}})-\mathsf{Y}^{\mathrm{C}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{y,z}}-\mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}})\\+\mathsf{X}^{\mathrm{C}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,y}}+\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,y}})-\mathsf{Y}^{\mathrm{C}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,y}}-\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,y}}).\end{aligned}\tag{8.9}$$

This Bell operator consists of a sum of three CHSH Bell operators. The correlations that we use for self-testing correspond to those which maximize $\left\langle\psi\right|\mathscr{B}\left|\psi\right\rangle$, which has maximum value $6\sqrt{2}$ (since each CHSH operator is upper bounded by $2\sqrt{2}$). This can be achieved by taking the following states and observables

$$\begin{gathered}\left|\psi\right\rangle=\left|\Phi^+\right\rangle=\frac{1}{\sqrt{2}}\left[\left|00\right\rangle+\left|11\right\rangle\right],\\ \mathsf{Z}^{\mathrm{C}}=\sigma_{\mathrm{Z}},\quad\mathsf{X}^{\mathrm{C}}=\sigma_{\mathrm{X}},\quad\mathsf{Y}^{\mathrm{C}}=\sigma_{yy},\\ \mathrm{D}^{\mathrm{A}_0}_{i,j}=\frac{\sigma_i+\sigma_j}{\sqrt{2}},\quad\mathrm{E}^{\mathrm{A}_0}_{i,j}=\frac{\sigma_i-\sigma_j}{\sqrt{2}},\end{gathered}\tag{8.10}$$

for $(i,j)=(z,x),(z,y),(x,y)$. The basic intuition of the self-testing is that since maximal violation of a single CHSH inequality requires anti-commuting qubit observables on a maximally entangled state [CHSH69], the maximum value of (8.9) should imply three mutually anti-commuting observables on the maximally entangled state, given by the three Pauli observables (or their transpositions). Indeed, we will see that this is the case.

One way to achieve this is to build a sum-of-squares (SOS) decomposition of the shifted Bell operator $6\sqrt{2}\mathbb{1}-\mathscr{B}$ of the form

$$6\sqrt{2}\mathbb{1}-\mathscr{B}=\sum_{\lambda}P_{\lambda}^{\dagger}P_{\lambda}.\tag{8.11}$$

Such a decomposition is given by

$$\begin{aligned}2\left(6\sqrt{2}\mathbb{1}-\mathscr{B}\right)=&\left[\mathsf{Z}^{\mathrm{C}}-\tfrac{1}{\sqrt{2}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,z}}+\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}})\right]^2+\left[\mathsf{X}^{\mathrm{C}}-\tfrac{1}{\sqrt{2}}(D^{\mathrm{A}_0}_{\mathrm{x,z}}-\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}})\right]^2+\\&+\left[\mathsf{Z}^{\mathrm{C}}-\tfrac{1}{\sqrt{2}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{y,z}}+\mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}})\right]^2+\left[\mathsf{Y}^{\mathrm{C}}+\tfrac{1}{\sqrt{2}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{y,z}}-\mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}})\right]^2+\\&+\left[\mathsf{X}^{\mathrm{C}}-\tfrac{1}{\sqrt{2}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,y}}+\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,y}})\right]^2+\left[\mathsf{Y}^{\mathrm{C}}+\tfrac{1}{\sqrt{2}}(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,y}}-\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,y}})\right]^2\end{aligned}\tag{8.12}$$

Here, the P_λ's are Hermitian and so $P_\lambda^\dagger P_\lambda = P_\lambda^2$. At maximal value one has $\langle\psi|\mathscr{B}|\psi\rangle = 6\sqrt{2}$ and so

$$\sum_\lambda \langle\psi| P_\lambda^\dagger P_\lambda |\psi\rangle = 0. \tag{8.13}$$

Since each term in the above is greater or equal to zero we have $P_\lambda|\psi\rangle = 0$ for all λ. Applying this to the SOS decomposition (8.12) gives

$$\mathsf{Z}^{\mathrm{C}}|\psi\rangle = \tfrac{1}{\sqrt{2}}[\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,z}} + \mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}}]|\psi\rangle = \tfrac{1}{\sqrt{2}}[\mathrm{D}^{\mathrm{A}_0}_{\mathrm{y,z}} + \mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}}]|\psi\rangle, \tag{8.14}$$

$$\mathsf{X}^{\mathrm{C}}|\psi\rangle = \tfrac{1}{\sqrt{2}}[\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,z}} - \mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}}]|\psi\rangle = \tfrac{1}{\sqrt{2}}[\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,y}} + \mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,y}}]|\psi\rangle, \tag{8.15}$$

$$\mathsf{Y}^{\mathrm{C}}|\psi\rangle = \tfrac{1}{\sqrt{2}}[\mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}} - \mathrm{D}^{\mathrm{A}_0}_{\mathrm{y,z}}]|\psi\rangle = \tfrac{1}{\sqrt{2}}[\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,y}} - \mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,y}}]|\psi\rangle. \tag{8.16}$$

Since for any two unitary observables G_1 and G_2, the composite observables $\frac{\mathsf{G}_1+\mathsf{G}_2}{\sqrt{2}}$ and $\frac{\mathsf{G}_1-\mathsf{G}_2}{\sqrt{2}}$ anti-commute by construction, from the above three equations it follows that on the support of state $|\psi\rangle$ observables $\mathsf{Z}^{\mathrm{C}}, \mathsf{X}^{\mathrm{C}}$ and Y^{C} mutually anti-commute:

$$\{\mathsf{Z}^{\mathrm{C}}, \mathsf{X}^{\mathrm{C}}\}|\psi\rangle = \{\mathsf{Z}^{\mathrm{C}}, \mathsf{Y}^{\mathrm{C}}\}|\psi\rangle = \{\mathsf{X}^{\mathrm{C}}, \mathsf{Y}^{\mathrm{C}}\}|\psi\rangle = 0. \tag{8.17}$$

The conditions (8.14) - (8.16) and (8.17) allow us to construct a local unitary which will give us our desired self-testing. This unitary can be understood via the circuit of Fig. 8.3, and is based on the swap gate introduced in [MYS14] and is the same as the circuit found in [McKM11]. The unitaries $\hat{\mathsf{Z}}^{\mathrm{A}_0}$, $\hat{\mathsf{X}}^{\mathrm{A}_0}$, $\hat{\mathsf{Y}}^{\mathrm{A}_0}$ are regularized versions of the operators

$$\mathsf{Z}^{\mathrm{A}_0} = \frac{\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,z}} + \mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}}}{\sqrt{2}}, \quad \mathsf{X}^{\mathrm{A}_0} = \frac{\mathrm{D}^{\mathrm{A}_0}_{\mathrm{x,z}} - \mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}}}{\sqrt{2}}, \quad \mathsf{Y}^{\mathrm{A}_0} = \frac{\mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}} - \mathrm{D}^{\mathrm{A}_0}_{\mathrm{y,z}}}{\sqrt{2}}.$$

For example, $\hat{\mathsf{Z}}^{\mathrm{A}_0}$ is obtained by setting all zero eigenvalues of $\mathsf{Z}^{\mathrm{A}_0}$ to one and then defining $\hat{\mathsf{Z}}^{\mathrm{A}_0} = \mathsf{Z}^{\mathrm{A}_0}|\mathsf{Z}^{\mathrm{A}_0}|^{-1}$. Using standard techniques (see Appendix A), these can be shown to act in the same way as the non-regularized versions. With this we are ready to present the first of our self-testing lemmas.

Lemma 9.5. *Let the state* $|\psi\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A}_0}$ *and* ± 1 *outcome observables* X^{C}, Y^{C}, Z^{C}, $D^{\mathrm{A}_0}_{\mathrm{x,z}}$, $\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}}$, $D^{\mathrm{A}_0}_{\mathrm{x,y}}$, $\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,y}}$, $D^{\mathrm{A}_0}_{\mathrm{y,z}}$, $\mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}}$ *satisfy*

$$\langle\psi|\mathscr{B}|\psi\rangle = 6\sqrt{2}. \tag{8.18}$$

Then there exist local auxiliary states $|00\rangle \in [\mathscr{H}^{\mathrm{C}''} \otimes \mathscr{H}^{\mathrm{C}'}] \otimes [\mathscr{H}^{\mathrm{A}_0''} \otimes \mathscr{H}^{\mathrm{A}_0'}]$ *and a local unitary* $U = U_{\mathrm{C}} \otimes U_{\mathrm{A}_0}$ *such that:*

$$U[|\psi\rangle \otimes |00\rangle] = |\mathrm{junk}\rangle \otimes |\Phi^+\rangle^{\mathrm{C}'\mathrm{A}_0'}, \tag{8.19}$$

$$U[\mathsf{X}^{\mathrm{C}}|\psi\rangle \otimes |00\rangle] = |\mathrm{junk}\rangle \otimes \sigma_{\mathrm{X}}^{\mathrm{C}'}|\Phi^+\rangle^{\mathrm{C}'\mathrm{A}_0'}, \tag{8.20}$$

$$U[\mathsf{Z}^{\mathrm{C}}|\psi\rangle \otimes |00\rangle] = |\mathrm{junk}\rangle \otimes \sigma_{\mathrm{Z}}^{\mathrm{C}'}|\Phi^+\rangle^{\mathrm{C}'\mathrm{A}_0'}, \tag{8.21}$$

$$U[\mathsf{Y}^{\mathrm{C}}|\psi\rangle \otimes |00\rangle] = \sigma_{\mathrm{Z}}^{\mathrm{C}''}|\mathrm{junk}\rangle \otimes \sigma_{\mathrm{Y}}^{\mathrm{C}'}|\Phi^+\rangle^{\mathrm{C}'\mathrm{A}_0'}, \tag{8.22}$$

where $|\text{junk}\rangle$ *takes the form*

$$|\text{junk}\rangle = |\text{junk}_0\rangle^{\text{CA}_0} \otimes |00\rangle^{\text{C}''\text{A}''_0} + |\text{junk}_1\rangle^{\text{CA}_0} \otimes |11\rangle^{\text{C}''\text{A}''_0}. \tag{8.23}$$

Note that the complex observable σ_Y has an additional σ_Z measurement on the C'' space, as expected from Def. 9.1. Hence, the measurement Y can be understood as first measuring σ_Z on the state $|\text{junk}\rangle$, whose outcome decides whether $\pm\sigma_\text{Y}$ is performed on the state $|\Phi^+\rangle$. The probability that the observables $\{\sigma_\text{X}, \sigma_\text{Y}, \sigma_\text{Z}\}$ are used rather than the transposed measurements $\{\sigma_\text{X}, -\sigma_\text{Y}, \sigma_\text{Z}\}$ is given by the probability to obtain $+1$ for the $\sigma_\text{Z}^{\text{C}''}$ measurement. This probability remains unknown since one does not know the precise form of $|\text{junk}\rangle$ from the self-testing correlations alone. The proof of Lemma 1 can be found in Appendix A.

8.2.2 Parallel self-testing of Pauli observables

The protocol described above can be extended to a parallel self-test. Here, our aim is to self-test the n-fold tensor product of the maximally entangled state $|\Phi^+\rangle^{\otimes n}$ (which itself is a maximally entangled state of dimension 2^n) and all combinations of n-fold tensor products of Pauli measurements for Charlie, i.e. $\sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \otimes \sigma_{i_n}$ for $i_j = x, y, z$. This is achieved by an n-fold maximal parallel violation of the Bell inequality used in Lemma 9.5. As a basis we use the techniques of [Col17], where parallel self-testing of σ_X and σ_Z observables on the maximally entangled state was proven. Besides [Col17], parallel self-testing of n-fold tensor products of maximally entangled pairs of qubits has been presented in [McK17] and [CN16], and in [WBMS16] for $n = 2$. This section can thus be seen as an extension of these results to all three Pauli observables. Although we use the term ‘self-testing’ here, we will see that simply performing the protocol of Lemma 9.5 in parallel does not lead to a self-test according to definition 9.1. In the following subsection we correct this by adding additional Bell state measurements between local subsystems.

The scenario we consider is as follows. Charlie and Alice share the state $|\psi\rangle \in \mathscr{H}^\text{C} \otimes \mathscr{H}^\text{A}$. Charlie has a choice of 3^n measurements collected into the vector $\mathbf{z} = (z_1, z_2, \cdots, z_n)$ with $z_i = 1, 2, 3$, and each measurement has 2^n possible outcomes given by $\mathbf{c} = (c_1, c_2, \cdots, c_n)$ with $c_i = \pm 1$. Similarly, Alice has a choice of 6^n measurements given by the vector $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ with $x_i = 1, 2, 3, 4, 5, 6$, each with 2^n possible outputs given by $\mathbf{a} = (a_1, a_2, \cdots, a_n)$ with $a_i = \pm 1$. Fixing a value of i we thus have three possible settings for Charlie and six for Alice, corresponding to the self-test of the previous section that we now perform in parallel. In order to achieve this we will define an analogous Bell operator to (8.9) for each value of i.

To this end, we denote Charlie’s and Alice’s measurement projectors by $\Pi^\text{C}_{\mathbf{c}|\mathbf{z}}$ and $\Pi^\text{A}_{\mathbf{a}|\mathbf{x}}$

respectively. We then define the following unitary observables for Charlie

$$\mathsf{O}_{i|\mathbf{z}} = \sum_{\mathbf{c}|c_i=+1} \Pi^{\mathrm{C}}_{\mathbf{c}|\mathbf{z}} - \sum_{\mathbf{c}|c_i=-1} \Pi^{\mathrm{C}}_{\mathbf{c}|\mathbf{z}}. \tag{8.24}$$

These operators can be understood as ±1 valued observables that depend on the output c_i only for a particular choice of input $\mathbf{z}$, and are thus analogous to one of the three Pauli measurements (given by the value z_i) acting on the i^{th} subspace of the maximally entangled state. Next we define the operators

$$\mathsf{Z}^{\mathrm{C}}_i = \frac{1}{3^{n-1}} \sum_{\mathbf{z}|z_i=1} \mathsf{O}_{i|\mathbf{z}}, \tag{8.25}$$

$$\mathsf{X}^{\mathrm{C}}_i = \frac{1}{3^{n-1}} \sum_{\mathbf{z}|z_i=2} \mathsf{O}_{i|\mathbf{z}}, \tag{8.26}$$

$$\mathsf{Y}^{\mathrm{C}}_i = \frac{1}{3^{n-1}} \sum_{\mathbf{z}|z_i=3} \mathsf{O}_{i|\mathbf{z}}, \tag{8.27}$$

that is, the average observables compatible with a particular choice of z_i.

Similarly for Alice we define the unitary observables

$$\mathrm{P}_{i|\mathbf{x}} = \sum_{\mathbf{a}|a_i=+1} \Pi^{\mathrm{A}_0}_{\mathbf{a}|\mathbf{x}} - \sum_{\mathbf{a}|a_i=-1} \Pi^{\mathrm{A}_0}_{\mathbf{a}|\mathbf{x}} \tag{8.28}$$

and the six operators

$$\begin{aligned}
\mathrm{D}^{\mathrm{A}_0}_{\mathrm{xz},i} &= \frac{1}{6^{n-1}} \sum_{\mathbf{x}|x_i=1} \mathrm{P}_{i|\mathbf{x}}, \quad \mathrm{E}^{\mathrm{A}_0}_{\mathrm{xz},i} = \frac{1}{6^{n-1}} \sum_{\mathbf{x}|x_i=2} \mathrm{P}_{i|\mathbf{x}},\\
\mathrm{D}^{\mathrm{A}_0}_{\mathrm{yz},i} &= \frac{1}{6^{n-1}} \sum_{\mathbf{x}|x_i=3} \mathrm{P}_{i|\mathbf{x}}, \quad \mathrm{E}^{\mathrm{A}_0}_{\mathrm{yz},i} = \frac{1}{6^{n-1}} \sum_{\mathbf{x}|x_i=4} \mathrm{P}_{i|\mathbf{x}},\\
\mathrm{D}^{\mathrm{A}_0}_{\mathrm{xy},i} &= \frac{1}{6^{n-1}} \sum_{\mathbf{x}|x_i=5} \mathrm{P}_{i|\mathbf{x}}, \quad \mathrm{E}^{\mathrm{A}_0}_{\mathrm{xy},i} = \frac{1}{6^{n-1}} \sum_{\mathbf{x}|x_i=6} \mathrm{P}_{i|\mathbf{x}}.
\end{aligned} \tag{8.29}$$

We now consider Bell operators of the form

$$\begin{aligned}
\mathscr{B}_i = {} & \mathsf{Z}^{\mathrm{C}}_i(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{xz},i} + \mathrm{E}^{\mathrm{A}_0}_{\mathrm{xz},i}) + \mathsf{X}^{\mathrm{C}}_i(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{xz},i} - \mathrm{E}^{\mathrm{A}_0}_{\mathrm{xz},i}) + \mathsf{Z}^{\mathrm{C}}_i(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{yz},i} + \mathrm{E}^{\mathrm{A}_0}_{\mathrm{yz},i}) - \mathsf{Y}^{\mathrm{C}}_i(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{yz},i} - \mathrm{E}^{\mathrm{A}_0}_{\mathrm{yz},i})\\
& + \mathsf{X}^{\mathrm{C}}_i(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{xy},i} + \mathrm{E}^{\mathrm{A}_0}_{\mathrm{xy},i}) - \mathsf{Y}^{\mathrm{C}}_i(\mathrm{D}^{\mathrm{A}_0}_{\mathrm{xy},i} - \mathrm{E}^{\mathrm{A}_0}_{\mathrm{xy},i}).
\end{aligned} \tag{8.30}$$

This is simply the Bell inequality (8.9), for the inputs z_i and x_i averaged over all compatible $\mathbf{z}$ and $\mathbf{x}$. One can thus obtain $\langle\psi|\mathscr{B}_i|\psi\rangle = 6\sqrt{2}$ for each i by taking n copies of the maximally entangled state of dimension two and adopting the previous measurement strategy (8.10) independently on each of the copies. From the observation of maximal violation for all i, a self-testing circuit (a parallel version of the circuit of Lemma 1) can be constructed, see Fig. B.1 in Appendix B. We then have the following lemma.

Lemma 9.6. *Let the state* $|\psi\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A_0}}$ *and operators* $\mathsf{Z}_i^{\mathrm{C}}$, $\mathsf{X}_i^{\mathrm{C}}$, $\mathsf{Y}_i^{\mathrm{C}}$, $D_{\mathrm{xz},i}^{\mathrm{A_0}}$, $\mathrm{E}_{\mathrm{xz},i}^{\mathrm{A_0}}$, $D_{\mathrm{yz},i}^{\mathrm{A_0}}$, $\mathrm{E}_{\mathrm{yz},i}^{\mathrm{A_0}}$, $D_{\mathrm{xy},i}^{\mathrm{A_0}}$, $\mathrm{E}_{\mathrm{xy},i}^{\mathrm{A_0}}$ *defined above satisfy*

$$\langle\psi|\mathscr{B}_i|\psi\rangle = 6\sqrt{2}, \tag{8.31}$$

for every $i \in \{1,\dots n\}$. *Then there exists a local unitary* $U = U_{\mathrm{C}} \otimes U_{\mathrm{A_0}}$, *local registers* $|00\rangle \in \otimes_{i=1}^{n}[\mathscr{H}^{\mathrm{C}_i''} \otimes \mathscr{H}^{\mathrm{C}_i'}] \otimes [\mathscr{H}^{\mathrm{A}_i''} \otimes \mathscr{H}^{\mathrm{A}_i'}]$ *and a normalized state* $|\xi\rangle$ *such that*

$$\begin{aligned}
U\left[|\psi\rangle \otimes |00\rangle\right] &= |\xi\rangle \otimes \left[\otimes_{i=1}^{n} |\Phi^{+}\rangle^{\mathrm{C}_i'\mathrm{A}_i'}\right], \\
U\left[\mathsf{Z}_j^{\mathrm{C}}|\psi\rangle \otimes |00\rangle\right] &= |\xi\rangle \otimes \left[\sigma_{\mathrm{Z}}{}^{\mathrm{C}_j'} \otimes_{i=1}^{n} |\Phi^{+}\rangle^{\mathrm{C}_i'\mathrm{A}_i'}\right], \\
U\left[\mathsf{X}_j^{\mathrm{C}}|\psi\rangle \otimes |00\rangle\right] &= |\xi\rangle \otimes \left[\sigma_{\mathrm{X}}{}^{\mathrm{C}_j'} \otimes_{i=1}^{n} |\Phi^{+}\rangle^{\mathrm{C}_i'\mathrm{A}_i'}\right], \\
U\left[\mathsf{Y}_j^{\mathrm{C}}|\psi\rangle \otimes |00\rangle\right] &= \sigma_{\mathrm{X}}{}^{\mathrm{C}_j''}|\xi\rangle \otimes \left[\sigma_{\mathrm{Y}}{}^{\mathrm{C}_j'} \otimes_{i=1}^{n} |\Phi^{+}\rangle^{\mathrm{C}_i'\mathrm{A}_i'}\right],
\end{aligned}$$

for every $j \in \{1,2,\dots n\}$, *where* $|\xi\rangle$ *takes the form*

$$|\xi\rangle = \sum_{\bar{q}} |\xi_{\bar{q}}\rangle^{\mathrm{CA_0}} \otimes |\bar{q}\bar{q}\rangle^{\mathrm{C''A_0''}} \tag{8.32}$$

and the sum is over all bit strings $\bar{q} = (0,1)^n$

The proof of the above Lemma can be found in Appendix B. Note that since the self-tested measurements are extremal then the above statement must hold not only for the operators Z_j, X_j, Y_j but for each of the observables $\mathsf{O}_{i|\mathbf{z}}$ appearing in their definition, which implies that the input z_i indeed corresponds to the desired Pauli measurement on the correct subspace. The measurement $\sigma_{\mathrm{Z}}{}^{\mathrm{C}_j''}$ on the state $|\xi\rangle$ again plays the role of deciding whether the measurement $\sigma_{\mathrm{Y}}{}^{\mathrm{C}_j'}$ or $-\sigma_{\mathrm{Y}}{}^{\mathrm{C}_j'}$ is performed on the maximally entangled state. However, note that due to the form of $|\xi\rangle$, this is not guaranteed to be correlated with the other measurements of σ_{Y} on different local subspaces. As a result, one cannot equate this freedom to a local transposition on *all* of Charlie's subsystems, as needed from definition 9.1. In the following section we show how to overcome this problem by introducing additional measurement for Alice.

8.2.3 Aligning reference frames

As mentioned, Lemma 9.6 suffers from one drawback, namely that the y direction for each of Charlie's local subsystems need not be aligned. For example, if we take the case $n = 2$, Lemma 9.6 gives four possibilities for Charlie's effective measurements on the maximally entangled state given by $\{\sigma_{\mathrm{X}}, \pm\sigma_{\mathrm{Y}}, \sigma_{\mathrm{Z}}\} \otimes \{\sigma_{\mathrm{X}}, \pm\sigma_{\mathrm{Y}}, \sigma_{\mathrm{Z}}\}$. The probability that each of these strategies is used is unknown and could, for example, be $\frac{1}{4}$ for each. In this case, when the first subsystem measures σ_{Y}, the second subsystem has equal probability to

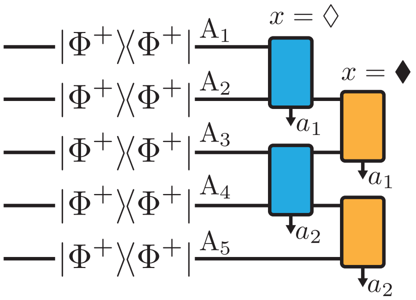
$|\Phi^+\rangle\langle\Phi^+|$
$|\Phi^+\rangle\langle\Phi^+|$
$|\Phi^+\rangle\langle\Phi^+|$
$|\Phi^+\rangle\langle\Phi^+|$
$|\Phi^+\rangle\langle\Phi^+|$
A_1
A_2
A_3
A_4
A_5
$x = \lozenge$
$x = \blacklozenge$
a_1
a_2
a_1
a_2

Figure 8.4: Graphical representation of the additional measurements performed by Alice for $x = \lozenge$ and $x = \blacklozenge$. Boxes between subspaces represent Bell state measurements.

measure either σ_Y or $-\sigma_Y$. This lack of alignment is an artefact from performing the protocol of Lemma 9.5 in parallel without trying to introduce any dependencies between the n individual self-tests. In the following we show that one can further restrict the the state $|\xi\rangle$ to be of the form

$$|\xi\rangle = |\xi_0\rangle \otimes |00\cdots 0\rangle^{C''A''_0} + |\xi_1\rangle \otimes |11\cdots 1\rangle^{C''A''_0} \tag{8.33}$$

by introducing additional Bell state measurements between subsystems of Alice. Since $|\xi\rangle$ now has only two terms, the flipping of the σ_Y measurements is always correlated; either none of the measurements are flipped (each subsystem measures σ_Y) or all the measurements are flipped (each subsystem measures $-\sigma_Y$). We note that a similar result was recently obtained in [CGJV17].

To illustrate the basic idea let us again consider the case $n = 2$, and assume we adopt the ideal measurement strategy (i.e. the strategy (8.10) in parallel). We now add an additional Bell state measurement for Alice which she performs on her two halves of the maximally entangled states. If Alice receives the outcome corresponding to the projector $|\Phi^+\rangle\langle\Phi^+|$, via entanglement swapping Charlie will hold the state $|\Phi^+\rangle$ in his local subsystem (for the other outcomes he will hold a different Bell state). This state has correlations $\langle\Phi^+|\,\sigma_X\otimes\sigma_X\,|\Phi^+\rangle = +1$, $\langle\Phi^+|\,\sigma_Y\otimes\sigma_Y\,|\Phi^+\rangle = -1$, $\langle\Phi^+|\,\sigma_Z\otimes\sigma_Z\,|\Phi^+\rangle = +1$. Hence, in order to reproduce these correlations, the direction of Charlie's two measurements of σ_Y need to be correlated as otherwise we would not have perfect anti-correlation for the measurement $\sigma_Y\otimes\sigma_Y$. In the following we formalize this intuition to strengthen Lemma 9.6 so that $|\xi\rangle$ is of the form (8.33).

The precise scenario we consider is the following. In addition to the 6^n measurements of Lemma 9.6 given by the vector $\mathbf{x}$, Alice has two extra measurements denoted by $x = \lozenge$ and $x = \blacklozenge$. These measurements have respectively 4^m and $4^{m'}$ outcomes, where $m = \lfloor \frac{n}{2} \rfloor$ and $m' = \lfloor \frac{n-1}{2} \rfloor$, which are grouped into the vectors $\mathbf{a} = (a_1, a_2, \cdots, a_m)$ and $\mathbf{a} = (a_1, a_2, \cdots, a_{m'})$ with $a_i = 0, 1, 2, 3$. We denote by $\Pi_{\mathbf{a},\lozenge}$ and $\Pi_{\mathbf{a},\blacklozenge}$ the projectors corre-

	$\mathbb{1}$	$\mathsf{Z}_{2l-1}\mathsf{Z}_{2l}$	$\mathsf{X}_{2l-1}\mathsf{X}_{2l}$	$\mathsf{Y}_{2l-1}\mathsf{Y}_{2l}$
$\mathsf{S}_{l,0}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$
$\mathsf{S}_{l,1}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$
$\mathsf{S}_{l,2}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
$\mathsf{S}_{l,3}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$

	$\mathbb{1}$	$\mathsf{Z}_{2l}\mathsf{Z}_{2l+1}$	$\mathsf{X}_{2l}\mathsf{X}_{2l+1}$	$\mathsf{Y}_{2l}\mathsf{Y}_{2l+1}$
$\mathsf{T}_{l,0}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$
$\mathsf{T}_{l,1}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$
$\mathsf{T}_{l,2}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
$\mathsf{T}_{l,3}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$

Table 8.1: Elements of the table give correlation $\langle\psi|C\otimes R|\psi\rangle$ where C is the operator labelling the column and R the operator labelling the row.

sponding to the outcomes of these measurements and define the projectors for $l = 1,\cdots,n$

$$\mathsf{S}_{l,a^*} = \sum_{\mathbf{a}:a_l=a^*} \Pi_{\mathbf{a}|\Diamond}, \quad \mathsf{T}_{l,a^*} = \sum_{\mathbf{a}:a_l=a^*} \Pi_{\mathbf{a}|\blacklozenge}, \tag{8.34}$$

that is, the projectors onto the the subspace corresponding to $a_l = a^*$ for the two measurements.

To generate our self-testing correlations we use the same strategy as Lemma 2 for the inputs $\mathbf{x}$ and $\mathbf{z}$. The two new measurements for Alice $x = \Diamond, \blacklozenge$ correspond to Bell state measurements between successive pairs of qubits of her system, where the Bell state measurements for the input $\blacklozenge$ are shifted with respect to those for $\Diamond$ (see Fig. 8.4). Specifically,

$$\Pi_{\mathbf{a},\Diamond} = \bigotimes_{l=1}^{\lfloor \frac{n}{2} \rfloor} |\Psi_{a_i}\rangle\langle\Psi_{a_i}|^{\mathrm{A}_{2l-1}\mathrm{A}_{2l}} \tag{8.35}$$

$$\Pi_{\mathbf{a},\blacklozenge} = \bigotimes_{l=1}^{\lfloor \frac{n-1}{2} \rfloor} |\Psi_{a_i}\rangle\langle\Psi_{a_i}|^{\mathrm{A}_{2l}\mathrm{A}_{2l+1}}, \tag{8.36}$$

where $\{|\Psi_0\rangle, |\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\} = \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$. With this choice, the correlations are given by Table 8.1, which follow from the correlations of the four Bell states. We are now ready for our final self-testing lemma (see Appendix C).

Lemma 9.7. *Let the state* $|\psi\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A}_0}$ *and* ± 1 *outcome observables* $\mathsf{X}^{\mathrm{C}}, \mathsf{Y}^{\mathrm{C}}, \mathsf{Z}^{\mathrm{C}}, D^{\mathrm{A}_0}_{\mathrm{x,z}}$, $\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,z}}, D^{\mathrm{A}_0}_{\mathrm{x,y}}$, $\mathrm{E}^{\mathrm{A}_0}_{\mathrm{x,y}}, D^{\mathrm{A}_0}_{\mathrm{y,z}}, \mathrm{E}^{\mathrm{A}_0}_{\mathrm{y,z}}$ *satisfy the conditions of Lemma 9.6 so that* $|\xi\rangle$ *has the form* (8.32)*. Furthermore, let projectors* S_{l,a^*} *and* T_{l,a^*} *satisfy the correlations given in Tables 8.1 for all l. Then* $|\xi\rangle$ *has the form*

$$|\xi\rangle = |\xi_0\rangle \otimes |0\ldots 0\rangle + |\xi_1\rangle \otimes |1\ldots 1\rangle \,. \tag{8.37}$$

Note that $|\xi\rangle$ now has the form of definition 9.1 as desired.

8.3 Entanglement certification

In this section we show how to make use of the preceding self-testing results to construct device-independent entanglement certification protocols for all bipartite entangled quantum states. The precise scenario that we consider is a quantum network featuring three bipartite states: ρ^{AB} shared between Alice and Bob, and two auxiliary states ρ^{CA_0} and $\rho^{\mathrm{B}_0\mathrm{D}}$ shared between Charlie and Alice, and Bob and Daisy respectively. Thus we have $\rho^{\mathrm{AB}} \in \mathbb{B}(\mathscr{H}^{\mathrm{A}} \otimes \mathscr{H}^{\mathrm{B}})$, $\rho^{\mathrm{CA}_0} \in \mathbb{B}(\mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A}_0})$ and $\rho^{\mathrm{B}_0\mathrm{D}} \in \mathbb{B}(\mathscr{H}^{\mathrm{B}_0} \otimes \mathscr{H}^{\mathrm{D}})$. We are interested in certifying the entanglement of the state ρ^{AB} when placed in a line network (see Fig. 8.1) featuring the auxillary states ρ^{CA_0} and $\rho^{\mathrm{B}_0\mathrm{D}}$. In such a network, the correlations $\{p(c,a,b,d|z,x,y,w)\}$ are given by:

$$p(c,a,b,d|z,x,y,w) = \operatorname{tr}\left[\left(\mathsf{M}^{\mathrm{C}}_{c|z} \otimes \mathsf{M}^{\mathrm{A}_0\mathrm{A}}_{a|x} \otimes \mathsf{M}^{\mathrm{BB}_0}_{b|y} \otimes \mathsf{M}^{\mathrm{D}}_{d|w}\right)\left(\rho^{\mathrm{CA}_0} \otimes \rho^{\mathrm{AB}} \otimes \rho^{\mathrm{B}_0\mathrm{D}}\right)\right], \tag{8.38}$$

where the $\mathsf{M}_{i|j}$ are the local measurement operators for each party. In the device-independent scenario, one only has access to the observed correlations $p(c,a,b,d|z,x,y,w)$. Hence, a device-independent certification of the entanglement of ρ^{AB} is possible only if the observed correlations cannot be reproduced by (8.38) for any separable ρ^{AB}. That is, one must show

$$p(c,a,b,d|z,x,y,w) \neq \operatorname{tr}\left[\left(\mathsf{M}'^{\mathrm{C}}_{c|z} \otimes \mathsf{M}'^{\mathrm{A}_0\mathrm{A}}_{a|x} \otimes \mathsf{M}'^{\mathrm{BB}_0}_{b|y} \otimes \mathsf{M}'^{\mathrm{D}}_{d|w}\right)\left(\rho'^{\mathrm{CA}_0} \otimes \rho^{\mathrm{AB}}_{\mathrm{SEP}} \otimes \rho'^{\mathrm{B}_0\mathrm{D}}\right)\right] \tag{8.39}$$

for any choice of separable $\rho^{\mathrm{AB}}_{\mathrm{SEP}}$, and any local measurement operators $\mathsf{M}'_{i|j}$ and auxillary states ρ'^{CA_0} and $\rho'^{\mathrm{B}_0\mathrm{D}}$. Note that the auxiliary states may be entangled and that since we impose no constraints on the dimension of the auxiliary systems in (8.39), we may purify them and take all measurements to be projective without loss of generality.

As we work in the device-independent scenario, all devices are treated as black boxes that process classical information. The precise assumptions we then make about the experiment are as follows.

1. States and measurements are described by quantum mechanics

2. The rounds of the experiment are independent and identically distributed (i.i.d.)
3. The network of Fig. 8.1 correctly describes the experimental setup

The first assumption is standard in device-independent studies. The second one appears in some cases and ideally one would like to drop it, but for simplicity we keep it here (see [DFR16, AFR16] for some recent progress) . The last assumption is required so that we may write our probabilities in the form (8.38). Physically this assumption means that one is able to prepare the three states independently and that they are trusted to interact in the way described by the network of Fig. 8.1 (for example the state ρ^{CA_0} should only interact with Charlie and Alice and not Bob or Daisy).

8.3.1 Certification protocols

We now present our entanglement certification protocols. These can be seen as a device-independent extension of the measurement device-independent entanglement witnesses (MDIEWs) presented in previous works [Bus12, BRLG13, Ver+16]. There, measurement devices are treated as black boxes, however inputs are given as a set of known informationally complete quantum states (in contrast to using classical variables as inputs). Then, an entanglement certification protocol can be built for every entangled state starting from an entanglement witness for the state. However, since this scheme requires a set of trusted input quantum states it is only partially device-independent. To see how these protocols can be made fully device-independent (i.e. how to remove the trust on the input states) consider that in the network of Fig. 8.1 the auxiliary states are given by maximally entangled states and that the complete set of projectors for Charlie's (resp. Daisy's) measurements form an informationally complete set. This can in fact be certified device-independently using the self-testing protocols of the first part of the chapter (see Lemma 9.5, Lemma 9.6 and Lemma 9.7). With this, the states that Alice (Bob) receives in the Hilbert space $\mathscr{H}^{\mathrm{A}_0}$ ($\mathscr{H}^{\mathrm{B}_0}$) conditioned on the different inputs and outputs of Charlie (Daisy) also form an informationally complete set. By interpreting these states as the inputs in a MDIEW protocol, one is essentially in the MDIEW scenario and the same techniques can be applied. Here, one has to be a bit careful due to the issue of transposition encountered in the self-testing sections, which we deal with in the supplementary material.

We now formalize this intuition and move to the main result of this section.

The entanglement of all bipartite entangled states can be certified device-independently in the network of Fig. 8.1.

In order to show this, we give an explicit family of entanglement certification protocols. The protocols we consider have the same structure for all states and are summarized as follows:

* **[generation of correlations]** The parties perform local measurements on their subsystems to obtain the correlations $p(c,a,b,d|z,x,y,w)$.

* The following is then verified:

  * **[self-testing]** The marginal distributions $p(c,a|z,x)$ and $p(b,d|y,w)$ maximally violate a Bell inequality that certifies that the auxiliary states each contain a maximally entangled state and that Charlie and Daisy each perform Pauli measurements on their subsystems.

  * **[entanglement certification]** The correlations violate an additional inequality

$$\mathscr{I}(p(c,a,b,d|z,x,y,w) \geq 0$$

that certifies ρ^{AB} is entangled.

For now, we have the unrealistic requirement that we have a maximum violation of a Bell inequality in step (ii). This can be weakened to allow for some noise on the statistics, which we discuss in the publication [BŠCA18a]. We now describe in detail the above protocol, starting with the case of two-qubit states.

8.3.2 Entanglement certification of all two-qubit entangled states

We start by defining the scenario in which we work. Charlie and Daisy both have a choice of three measurements $z,w = 1,2,3$ and Alice and Bob both have a choice of seven inputs $x,y = 1,2,3,4,5,6,\star$. All outputs are ± 1 valued.

(i) Generation of correlations— To generate the correlations in step (i) of the protocol, the parties chose $\rho^{\mathrm{CA_0}} = \rho^{\mathrm{B_0}D} = |\Phi^{+}\rangle\langle\Phi^{+}|$. Measurements for inputs $z = 1,2,3$ and $x = 1,\cdots,6$ for Charlie and Alice should be chosen so that the conditions of Lemma 9.5 are satisfied, i.e. given by the qubit observables

$$\sigma_{\mathrm{Z}},\, \sigma_{\mathrm{X}},\, \sigma_{\mathrm{Y}} \quad z = 1,2,3 \tag{8.40}$$

$$\frac{\sigma_{\mathrm{Z}} \pm \sigma_{\mathrm{X}}}{\sqrt{2}}, \frac{\sigma_{\mathrm{Z}} \pm \sigma_{\mathrm{Y}}}{\sqrt{2}}, \frac{\sigma_{\mathrm{X}} \pm \sigma_{\mathrm{Y}}}{\sqrt{2}} \quad x = 1,\cdots 6 \tag{8.41}$$

acting on the $\mathscr{H}^{\mathrm{C}}$ and $\mathscr{H}^{\mathrm{A_0}}$ spaces respectively. Measurements for Daisy and Bob are defined analogously. Lastly, the measurement operators for inputs $x = \star$, $y = \star$ are projections onto the maximally entangled state:

$$\mathsf{M}^{\mathrm{AA_0}}_{+|\star} = \mathsf{M}^{\mathrm{B_0B}}_{+|\star} = |\Phi^{+}\rangle\langle\Phi^{+}|. \tag{8.42}$$

(ii) Self-testing— Our next step is to define the Bell inequality used in step (ii) of the protocol. Here we focus on Charlie and Alice; the Bell inequality used by Daisy and Bob is the same. The inequality we consider is constructed by combining three CHSH Bell inequalities [CHSH69]. Define the expectation value for inputs z, x as

$$E_{z,x} = \sum_{c,a=\pm 1} c \cdot a \, p(c,a|z,x). \tag{8.43}$$

We then define the triple CHSH Bell inequality

$$\begin{aligned}\mathscr{J} = E_{1,1} + E_{1,2} + E_{2,1} - E_{2,2} \\ + E_{1,3} + E_{1,4} - E_{3,3} + E_{3,4} \\ + E_{2,5} + E_{2,6} - E_{3,5} + E_{3,6}.\end{aligned} \tag{8.44}$$

Note that each line in the above is a CHSH inequality, and each of Charlie's inputs appears in two of the lines, and that at this stage the inputs $x, y = \star$ remain unused. Using the states and measurements above one finds $\mathscr{J} = 6\sqrt{2}$. Via Lemma 9.5, this provides a self-test of the auxiliary states and measurements of Charlie and Daisy defined in step (i), up to local transposition. While our protocol is based on 'chaining' CHSH inequality, any other self-test of the maximally entangled pair of qubits and three Paili observables would work as well.

Entanglement certification— Our next task is to construct the inequality used in the final step of the protocol. The inequality is constructed from an entanglement witness $\mathscr{W}$ for the state ρ^{AB}. We thus have $\mathrm{tr}[\mathscr{W}\sigma] \geq 0$ for all separable states σ and $\mathrm{tr}[\mathscr{W}\rho^{\mathrm{AB}}] < 0$. Consider the projectors $\pi_{c|z} = \frac{1}{2}[\mathbb{1} + c\,\sigma_{\mathrm{Z}}]$ with $c = \pm 1$ and $z = 1,2,3$, that is, projectors onto the plus and minus eigenspaces of the Pauli operators. Since these form an (over-complete) basis of the set of Hermitian matrices, any entanglement witness may be decomposed as

$$\mathscr{W} = \sum_{cdzw} \omega_{cd}^{zw} \, \pi_{c|z} \otimes \pi_{d|w}. \tag{8.45}$$

To define our inequality, we make use of the additional inputs for both Alice and Bob $x = \star$ and $y = \star$. The inequality is then given by

$$\mathscr{I} = \sum_{cdzw} \omega_{cd}^{zw} \, p(c,+,+,d|z,x=\star,y=\star,w) \geq 0 \tag{8.46}$$

and is satisfied for all separable states but violated using ρ^{AB}. We first show that one can achieve $\mathscr{I} < 0$ for entangled $\rho^{\rangle\mathrm{B}}$. Using the states and measurements defined above one has

$$p(c,+,+,d|z,x=\star,y=\star,w) = \tag{8.47}$$

$$\mathrm{tr}\left[\pi_{c|z} \otimes |\Phi^{+}\rangle\langle\Phi^{+}| \otimes |\Phi^{+}\rangle\langle\Phi^{+}| \otimes \pi_{d|w} \, |\Phi^{+}\rangle\langle\Phi^{+}| \otimes \rho^{\mathrm{AB}} \otimes |\Phi^{+}\rangle\langle\Phi^{+}|\right]$$

$$= \frac{1}{4}\,\mathrm{tr}\left[|\Phi^{+}\rangle\langle\Phi^{+}| \otimes |\Phi^{+}\rangle\langle\Phi^{+}| \, \pi_{c|z}^{T} \otimes \rho^{\mathrm{AB}} \otimes \pi_{d|w}^{T}\right] \tag{8.48}$$

$$= \frac{1}{16}\,\mathrm{tr}\left[\pi_{c|z} \otimes \pi_{d|w} \, \rho^{\mathrm{AB}}\right], \tag{8.49}$$

where we have used $\mathrm{tr}_{\mathrm{A}}[|\Phi^{+}\rangle\langle\Phi^{+}|\,\pi^{\mathrm{A}}_{i|j}\otimes\mathbb{1}] = \frac{1}{2}\pi^{T}_{i|j}$ in the third and fourth line. One thus has

$$\mathscr{I} = \frac{1}{16}\sum_{czdw}\omega^{zw}_{cd}\,\mathrm{tr}[\pi_{c|z}\otimes\pi_{d|w}\,\rho^{\mathrm{AB}}] \tag{8.50}$$

$$\mathscr{I} = \frac{1}{16}\,\mathrm{tr}[\mathscr{W}\rho^{\mathrm{AB}}] < 0, \tag{8.51}$$

which follows from the fact that $\mathscr{W}$ is an entanglement witness for the state.

For separable sates, one sees that if the auxiliary states and measurements the same as above, then from (8.51) one has $\mathscr{I}\geq 0$ from the fact that $\mathscr{W}$ is an entanglement witness. Moreover, one can show that given maximal violations of (8.44) in the previous part of the protocol, then for any auxiliary states and measurements one has

$$\mathscr{I} = \mathrm{tr}\left[\mathscr{W}\,\Lambda(\rho^{\mathrm{AB}})\right], \tag{8.52}$$

where Λ is a local, positive map on separable quantum states and so $\mathscr{I}\geq 0$ (see Appendix D.1). A crucial observation in the proof of the above is that although the measurements for Charlie and Daisy are only certified via self-testing up to a possible transposition, this uncertainty can be mapped to possible local transpositions on the state ρ^{AB}. Since local transpositions map separable states to separable states, this then allows for the same technique as [BRLG13] to be applied. More precisely, in some instances the witness $\mathscr{W}$ is measured, and in other the witness $\mathscr{W}^{T_A}$ is measured instead. But given that

$$\mathrm{tr}\left[\mathscr{W}\rho_{\mathrm{sep}}\right] > 0,$$

it also holds

$$\mathrm{tr}\left[\mathscr{W}^{T_A}\rho_{\mathrm{sep}}\right] = \mathrm{tr}\left[\mathscr{W}\rho^{T_A}_{\mathrm{sep}}\right] > 0,$$

because $\rho^{T_A}_{\mathrm{sep}}$ must be separable.

8.3.3 Entanglement certification of high dimensional states

The previous protocol for two-qubit states can be applied in parallel to construct entanglement certification protocols for bipartite states of any dimension. In the following we construct protocols for states of local dimension 2^n where $n = 2,3,\cdots$. Since a state of local dimension d can be seen as a particular case of a state of dimension 2^n for some $n\geq\log_2 d$ this implies a protocol for any dimension.

The scenario we consider is as follows. Charlie and Daisy each have 3^n inputs, given by the vectors $\mathbf{z} = (z_1,\cdots,z_n)$ and $\mathbf{w} = (w_1,\cdots,w_n)$ with $z_i,w_i = 1,2,3$, each with 2^n outcomes given by $\mathbf{c} = (c_1,\cdots,c_n)$ and $\mathbf{d} = (d_1,\cdots,d_n)$ with $c_i,d_i = \pm 1$. Alice and Bob each have 6^n inputs given by the vectors $\mathbf{x} = (x_1,\cdots,x_n)$, $\mathbf{y} = (y_1,\cdots,y_n)$ with $x_i,y_i = 1,\cdots,6$, with outcomes $\mathbf{a} = (a_1, \cdots, a_n)$, $\mathbf{b} = (b_1, \cdots, b_n)$ with $a_i, b_i = \pm 1$. Further to this Alice and Bob have each two additional inputs $x = \lozenge, \blacklozenge$ and $y = \lozenge, \blacklozenge$ with $4^{\lfloor \frac{n}{2} \rfloor}$ and $4^{\lfloor \frac{n-1}{2} \rfloor}$ outputs respectively (as in Lemma 9.7), and inputs $x = \star$ and $y = \star$ with outputs $a = \pm 1$, $b = \pm 1$ (to be used in step (iii) of the protocol).

(*) *Generation of correlations*— Since we will perform the previous protocol in parallel, the Hilbert spaces of the auxiliary systems are written as the tensor product of n qubit spaces: $\mathscr{H}^{\mathrm{C}} = \otimes_i \mathscr{H}^{\mathrm{C}_i}$, $\mathscr{H}^{\mathrm{A}_0} = \otimes_i \mathscr{H}^{\mathrm{A}_i}$ (and similarly for Daisy, Bob). The auxiliary states are then n-fold tensors of maximally entangled states on each two-qubit subspace:

$$\rho^{\mathrm{CA}_0} = \otimes_{i=1}^{n} |\Phi^+\rangle\langle\Phi^+|^{\mathrm{C}_i\mathrm{A}_i}; \quad \rho^{\mathrm{B}_0 D} = \otimes_{i=1}^{n} |\Phi^+\rangle\langle\Phi^+|^{\mathrm{B}_i D_i}.$$

Measurements are a parallel version of the measurements (8.40), (8.41), i.e. they are given by n-fold tensor products of the measurements (8.40), (8.41), acting on each maximally entangled state. For example $z_i = 1, 2, 3$ corresponds to a measurement of $\sigma_{\mathrm{Z}}, \sigma_{\mathrm{X}}, \sigma_{\mathrm{Y}}$ on the i^{th} subsystem of Charlie with outcome c_i. As before, the measurements $\mathsf{M}_{+|\star}$ are projections onto the maximally entangled state:

$$\mathsf{M}_{+|\star}^{\mathrm{AA}_0} = \mathsf{M}_{+|\star}^{\mathrm{B}_0\mathrm{B}} = |\Phi^+\rangle\langle\Phi^+| \tag{8.53}$$

where here $|\Phi^+\rangle = \frac{1}{\sqrt{2^n}} \sum_i |ii\rangle \in \mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A}_0}$. Finally, the measurements for the inputs $x, y = \lozenge, \blacklozenge$ are chosen to be tensor products of Bell state measurements between successive pairs of qubits of the local subsystems of Alice and Bob, and where the Bell state measurements for the input $\lozenge$ are shifted with respect to those for $\blacklozenge$ (see Fig. 8.4 and Section 8.2.3 for more details).

(**) *Self-testing*— The Bell inequality is now a parallel version of (8.44) (again we just describe the inequality for Charlie and Alice). Define the average expectation value for the bits c_i, a_i given $z_i = z$, $x_i = x$ as

$$E^i_{z,x} = \frac{1}{3^{n-1} 6^{n-1}} \sum_{\substack{\mathbf{z}|z_i = z \\ \mathbf{x}|x_i = x}} \sum_{\mathbf{c},\mathbf{a}} c_i \cdot a_i \, p(\mathbf{c}, \mathbf{a} | \mathbf{z}, \mathbf{x}). \tag{8.54}$$

For each i, we now have the triple CHSH Bell inequality:

$$\begin{aligned} \mathscr{J}_i = E^i_{1,1} + E^i_{1,2} + E^i_{2,1} - E^i_{2,2} & \\ + E^i_{1,3} + E^i_{1,4} - E^i_{3,3} + E^i_{3,4} & \\ + E^i_{2,5} + E^i_{2,6} - E^i_{3,5} + E^i_{3,6}. & \end{aligned} \tag{8.55}$$

For the entanglement certification protocol we require maximum violation of each of these inequalities, i.e.

$$\sum_{i=1}^{n} \mathscr{J}_i = n \cdot 6\sqrt{2}. \tag{8.56}$$

We further require that the measurements $x,y = \lozenge, \blacklozenge$ correctly reproduce the Bell state measurement correlations given in tables 8.1, which is achieved by our chosen measurement strategy and detailed in section 8.2.3. With these conditions met, we may apply Lemma 9.7 and move on to the entanglement certification of ρ^{AB}.

(***)*Entanglement certification*— Similarly to (8.45), we may decompose an entanglement witness for $\rho^{\mathrm{AB}} \in \otimes_i[\mathscr{H}^{\mathrm{A}_i} \otimes \mathscr{H}^{\mathrm{B}_i}]$ using tensor products of Pauli projectors as an (over-complete) basis:

$$\mathscr{W} = \sum_{\mathbf{c},\mathbf{d},\mathbf{z},\mathbf{w}} \omega_{\mathbf{cd}}^{\mathbf{zw}} \otimes_i \left[\pi_{c_i|z_i}^{\mathrm{A}_i} \otimes \pi_{d_i|w_i}^{\mathrm{B}_i}\right]. \tag{8.57}$$

The inequality that is used to certify entanglement is then

$$\mathscr{I} = \sum_{\mathbf{c},\mathbf{d},\mathbf{z},\mathbf{w}} \omega_{\mathbf{cd}}^{\mathbf{zw}} p(\mathbf{c},+,+,\mathbf{d}|\mathbf{z}, x=\star, y=\star, \mathbf{w}) \geq 0, \tag{8.58}$$

which for separable states gives

$$\mathscr{I} = \mathrm{tr}\left[\mathscr{W}\,\Lambda(\rho^{\mathrm{AB}})\right] \geq 0, \tag{8.59}$$

where Λ is again a local positive map on separable states (see supplementary material D.2 for a full proof). Note here that simply using two-qubit strategy in parallel (i.e. using Lemma 9.6) without the additional Bell state measurements for inputs $x,y = \lozenge, \blacklozenge$ would lead to problems. This is because the measurements for Charlie and Daisy would be certified only up to possible flipping of any number of their n σ_{Y} measurements. When mapping this uncertainty to the state ρ^{AB}, this corresponds to possible local transposition on *part of a local subsystem* of ρ^{AB}, which may map separable states to unphysical (non-positive) states. Hence, the additional Bell state measurements ensure that either none or all σ_{Y} measurements are flipped, corresponding to a transposition of the entire local subsystem of ρ^{AB} so that the map Λ is positive on separable states.

Finally, we show that $\mathscr{I}$ is violated by ρ^{AB}. Using the measurement strategy above and that $\mathrm{tr}_{\mathrm{A}}[|\Phi^+\rangle\langle\Phi^+|\,\pi_{i|j}^{\mathrm{A}} \otimes \mathbb{1}] = \frac{1}{d}\pi_{i|j}^{T}$ for the maximally entangled state of dimension d, it is straightforward to show using the same technique as (8.47) - (8.49) that

$$\mathscr{I} = \frac{1}{d^4} \sum_{\mathbf{c},\mathbf{d},\mathbf{z},\mathbf{w}} \omega_{\mathbf{cd}}^{\mathbf{zw}}\, \mathrm{tr}\left[\otimes_i \left(\pi_{c_i|u_i}^{\mathrm{A}_i} \otimes \pi_{d_i|w_i}^{\mathrm{B}_i}\right) \rho^{\mathrm{AB}}\right] \tag{8.60}$$

$$= \frac{1}{d^4}\,\mathrm{tr}\left[\mathscr{W}\rho^{\mathrm{AB}}\right] < 0, \tag{8.61}$$

thus certifying the entanglement of ρ^{AB}.

8.4 Discussion

We have shown that all bipartite entangled quantum states are capable of producing correlations that cannot be obtained using separable states by placing them in a larger network of auxiliary states and using tools from self-testing and measurement device-independent entanglement witnesses. It is desirable to strengthen the self-testing part of our protocol; in particular, improved robustness bounds for self-testing would immediately translate into better noise-tolerance of our protocols. One would most likely be able to achieve this using the protocols presented in [CGJV17] where self-testing statements for Pauli observables are presented with a robustness scaling that is independent of n. Furthermore, the choice of measurements used for self-testing could be made much more efficient. In general, one needs d^2 linearly independent projectors to form an informationally complete set, however for local dimension 2^n we make use of an over-complete basis of 6^n projectors (coming from the tensor product of Pauli projectors), a difference that is exponential in n. Hence, a more efficient self-test of informationally complete sets of measurements would improve the efficiency of the protocol. Furthermore, given a particular state, one typically does not need the full set of projectors in order to write an entanglement witness for the state. It would therefore be interesting to study self-testing protocols that certify only those projectors that appear in a particular decomposition of an entanglement witness.

Although we have focused on the task of entanglement certification, our technique can in principle be applied to other convex sets of quantum states other than the separable set where linear witnesses can also be used. Due to the ambiguity of local unitaries and local transpositions in the self-testing part of our protocol, such sets would need to be closed under local unitary operations and local transpositions (as is the case for the separable set). For example, one could apply the same technique to certify entangled states with negative partial transpose. Finally, it would also be interesting to investigate the possibility of using our general technique for other device-independent tasks, for example using similar ideas to [LPTRG13, LCQ12, BP12] to construct device-independent quantum key distribution protocols, or to generalize our protocol for the certification of genuine multipartite entanglement.

Chapter 9

Conclusion and outlook

The main topic of this thesis is the certification of quantum resources which can be used in quantum information protocols. Anticipating the significance quantum devices will have in cryptographic and computational tasks, it is crucially important to build reliable certification techniques. In any certification task the first step is the choice of initial assumptions. Since quantum information protocols are usually subject to various kinds of adversarial activities, the fewer the assumptions about a device to be certified, the stronger the certification. In such circumstances the device-independent scenario gained a lot of attention as it relies on a very small amount of reasonable assumptions. In the first part of this thesis we explored one of the most fundamental device-independent protocols, that of self-testing, i.e. the device-independent certification of a certain quantum state. In the second part we considered the certification of quantum resources centred around a relaxation of the device-independent scenario, the so-called measurement-device-independent scenario. We explored ways to estimate the amount of entanglement in this scenario and later, by connecting these results to self-testing, we suggested a protocol for the device-independent detection of all entangled states. We also identified quantum state teleportation as a native measurement-device-independent protocol and explored its properties from this new point-of-view. In this last chapter we briefly recall the achieved results, outline their significance and discuss the open questions and directions for future research.

Self-testing

When it comes to self-testing our aim was to find new self-testing protocols and extend the validity of the known ideas in unexplored regions. Going in that direction in Chapter 3 we proved that chained Bell inequalities can be used to robustly self-test a maximally entangled pair of qubits and a large class of real quantum measurements. The self-testing proof is largely based on the 2nd order SOS decomposition of the shifted chained Bell operator. This result enabled to prove that chained Bell inequalities are useful for randomness generation, as conjectured in previous works. Though our self-testing protocol is proven to be robust, the robustness bounds get worse when the number of measurements increases. To make our protocol more useful for practical purposes the imminent aim would be to improve the scaling of robustness bounds with the number of inputs. The authors of [BKP06] introduced a generalisation of chained Bell inequalities that is maximally violated by the maximally entangled pair of qudits. It would be interesting to see if our self-testing protocol generalizes to this class of Bell inequalities.

Another research direction presented in this thesis is the self-testing of multipartite quantum states, presented in Chapter 4. Prior to our work, not much was known about this topic. We showed that the method previously used to self-test tripartite W-state can be used to self-test large classes of multipartite qubit states. Furthermore, we used the extension of this method to formulate the first self-test of a multipartite qudit state. A natural question is if this method extends its validity to self-testing of arbitrary multipartite pure entangled quantum states. It seems that for a generic state without any symmetries the number of measurements necessary for self-testing would increase polynomially with the number of parties. A big challenge is to understand if it is possible to self-test such non-symmetric states with a constant number of measurements.

Finally, in Chapter 5 we explored the properties of self-testing in the semi-device-independent scenario native to EPR steering. We defined two approaches to self-testing in this scenario, correlation-based and assemblage-based, and compared their performance to that of standard device-independent self-testing. While analytical bounds scale better in semi-device-independent scenario, the assymptotical behaviour of the robustness bounds is the same as for device-independent protocols, i.e. the improvement is constant. However, analytical proofs tend to be simpler and we believe that exploring self-testing in steering scenarios can be used as an intermediate step towards solving some difficult questions in standard self-testing protocols. For example, finding truly robust self-testing protocols for high-dimensional bipartite quantum states seems to be a difficult problem. Exploring semi-device-independent variant could give valuable insights in what can be achieved. Notably, it would give lower bounds on the robustness of device-independent protocol, since the robustness in the semi-device-independent scenario can only be better.

Certification of quantum resources and measurement-device-independent scenario

Certification tasks can be done device-independently whenever the system under consideration exhibits nonlocal correlations. For example, device-independent entanglement detection relies on the violation of a Bell inequality. However, since not all entangled states violate Bell inequalities not all of them can be detected in a device-independent manner. A solution to this problem came through the measurement-device-independent (MDI) scenario. In Chapter 6 we went a step further from just detecting bipartite entanglement and discussed the quantification of entanglement in the MDI scenario. We showed how one can put a lower bound on the entanglement negativity and robustness of entanglement present in quantum networks. Besides entanglement, we explored how the

MDI scenario affects randomness generation. Contrarily to the device-independent scenario, we showed that in the MDI scenario randomness generation is not tied to nonlocal correlations but to the inability of an eavesdropper to perfectly distinguish quantum states that the parties use as inputs to their black boxes. In accordance with this, we proved that randomness can be generated from single party experiments and in bipartite experiments even from separable states. There are several directions for future research related to the results presented in Chapter 6. Going beyond detecting and quantifying entanglement in the MDI scenario it may be of interest to explore certification of quantum states, i.e. MDI variant of self-testing. When it comes to randomness generation it is interesting to see how MDI randomness generation compares to the other semi-device-independent randomness generation protocols. Finally, we explored the case when parties have fully characterized preparation devices. One may wonder how the security proofs are affected if we consider a situation in which the parties prepare characterized mixed states but an eavesdropper might hold the purifications.

The topic of Chapter 8 is closely related to the topic of Chapter 6. Since all entangled states can be detected in the MDI scenario, the main idea of Chapter 8 is to make MDI detection of entanglement witnessing device-independent. This can be done with the aid of the main subject of the first part of the thesis, self-testing. Two parties, Alice and Bob, want their quantum states which they use as quantum inputs to be prepared by two additional spatially distant parties, Charlie and Daisy. This is possible if Alice and Bob share with Charlie and Daisy maximally entangled pairs of qudits. By applying the appropriate measurement on their share of maximally entangled pairs Charlie and Daisy can conveniently steer Alice's and Bob's shares which they later use as quantum inputs. Self-testing methods are employed to ensure that Charlie and Daisy apply projective measurements on maximally entangled pairs of qudits. In this way, any entangled bipartite state when put in a small quantum network consisting of four parties can produce overal conditional probability distributions which cannot be reproduced by any separable state. There are several open questions regarding the topic of device-independent detection of all entangled states and the method presented in Chapter 8. Right away, it would be useful to explore the robustness of the protocol and to try to make the whole method closer to potential experimental applications. The bottleneck of all considerations regarding the presence of noise and experimental imperfections is the robustness of the self-testing part of the protocol. When it comes to the application of our methods it would be very interesting to see if similar methods can be used for the (measurement-)device-independent detection of Gaussian entangled states. Another MDI protocol where our methods could be useful is measurement-device-independet quantum key distribution.

Finally, in Chapter 7 we discussed various aspects of the quantum state teleportation. The crux of the whole chapter is identifying quantum state teleportation as a one-sided measurement-device-independent protocol. This insight allowed us to apply well-known methods from the MDI scenario to the study of teleportation. The main insight is that all entangled states are capable of producing teleportation data which cannot be simulated with classically correlated states. This is in clear contrast with previous approaches to characterising the non-classicality of teleportation based on the average teleportation fidelity. According to that benchmark some classes of entangled states, among which are all bound entangled states, are useless for teleportation. We provided an semi-definite-programming optimization which checks if there is a classical simulation of the given teleportation data. The dual form of provides a teleportation witness, whose violation indicates the non-classicality of the teleportation protocol. Furthermore, we introduced ways to quantify the non-classicality of teleportation. The introduced teleportation quantifiers can be used to put a lower bound on several entanglement measures, such as entanglement negativity, robustness of entanglement or the best separable approximation. The first open question related to the results presented in Chapter 7 is whether similar methods can be used to characterize the non-classicality of continuous variable teleportation. Finally, we are interested to explore the fundamental role of entanglement in more complicated protcols based on teleportation such as measurement-based quantum computing or quantum repeaters.

Appendices

Appendix A

Proof of Lemma 9.5

In this section we prove Lemma 9.5 from the main text. Define the following operators:

$$Z^{A_0}_{x,z} = \frac{D^{A_0}_{x,z} + E^{A_0}_{x,z}}{\sqrt{2}}, \quad X^{A_0}_{x,z} = \frac{D^{A_0}_{x,z} - E^{A_0}_{x,z}}{\sqrt{2}}, \quad Z^{A_0}_{y,z} = \frac{D^{A_0}_{y,z} + E^{A_0}_{y,z}}{\sqrt{2}},$$

$$Y^{A_0}_{y,z} = \frac{D^{A_0}_{y,z} - E^{A_0}_{y,z}}{\sqrt{2}}, \quad X^{A_0}_{x,y} = \frac{D^{A_0}_{x,y} - E^{A_0}_{x,y}}{\sqrt{2}}, \quad Y^{A_0}_{x,y} = \frac{D^{A_0}_{x,y} + E^{A_0}_{x,y}}{\sqrt{2}}. \tag{A.1}$$

From the (8.14) – (8.16) we have

$$Z^{A_0}_{x,z} |\psi\rangle = Z^{A_0}_{y,z} |\psi\rangle, \quad X^{A_0}_{x,z} |\psi\rangle = X^{A_0}_{x,y} |\psi\rangle, \quad Y^{A_0}_{y,z} |\psi\rangle = Y^{A_0}_{x,y} |\psi\rangle. \tag{A.2}$$

Hence, defining

$$Z^{A_0} \equiv Z^{A_0}_{x,z}, \quad X^{A_0} \equiv X^{A_0}_{x,z}, \quad Y^{A_0} \equiv Y^{A_0}_{y,z} \tag{A.3}$$

we have from (8.14) – (8.17) the conditions

$$Z^{C} |\psi\rangle = Z^{A_0} |\psi\rangle, \quad X^{C} |\psi\rangle = X^{\rangle} |\psi\rangle, \quad Y^{C} |\psi\rangle = -Y^{A_0} |\psi\rangle, \tag{A.4}$$

$$\{Z^{C}, X^{C}\} |\psi\rangle = 0, \quad \{Z^{C}, Y^{C}\} |\psi\rangle = 0, \quad \{Y^{C}, X^{C}\} |\psi\rangle = 0, \tag{A.5}$$

$$\{Z^{A_0}, X^{A_0}\} |\psi\rangle = 0, \quad \{Z^{A_0}, Y^{A_0}\} |\psi\rangle = 0, \quad \{Y^{A_0}, X^{A_0}\} |\psi\rangle = 0. \tag{A.6}$$

Note that the operators Z^{A_0}, X^{A_0}, Y^{A_0} are not necessarily unitary. We may define the regularized versions of these operators $\hat{Z}^{A_0}$, $\hat{X}^{A_0}$, $\hat{Y}^{A_0}$ which are obtained from the original operators by renormalising all eigenvalues to ±1 and setting any zero eigenvalues to 1 (without changing the eigenvectors). Using standard techniques (for example see [**?** ŠASA16]) one can show that the regularized operators respect the same conditions, that is,

$$Z^{C} |\psi\rangle = \hat{Z}^{A_0} |\psi\rangle, \quad X^{C} |\psi\rangle = \hat{X}^{A_0} |\psi\rangle, \quad Y^{C} |\psi\rangle = -\hat{Y}^{A_0} |\psi\rangle, \tag{A.7}$$

$$\{Z^{C}, X^{C}\} |\psi\rangle = 0, \quad \{Z^{C}, Y^{C}\} |\psi\rangle = 0, \quad \{Y^{C}, X^{C}\} |\psi\rangle = 0, \tag{A.8}$$

$$\{\hat{Z}^{A_0}, \hat{X}^{A_0}\} |\psi\rangle = 0, \quad \{\hat{Z}^{A_0}, \hat{Y}^{A_0}\} |\psi\rangle = 0, \quad \{\hat{Y}^{A_0}, \hat{X}^{A_0}\} |\psi\rangle = 0. \tag{A.9}$$

Let us prove the first equality from (A.7), the other two being analogous. The following chain of equalities is satisfied

$$\begin{aligned}||(\hat{\mathsf{Z}}^{\mathrm{A_0}} - \mathsf{Z}^{\mathrm{A_0}})\,|\psi\rangle\,|| &= ||(\mathbb{1} - (\hat{\mathsf{Z}}^{\dagger})^{\mathrm{A_0}}\mathsf{Z}^{\mathrm{A_0}})\,|\psi\rangle\,|| = ||(\mathbb{1} - |\mathsf{Z}^{\mathrm{A_0}}|)\,|\psi\rangle\,|| \\ &= ||(\mathbb{1} - |\mathsf{Z}^{\mathrm{C}}\mathsf{Z}^{\mathrm{A_0}}|)\,|\psi\rangle\,|| \leq ||(\mathbb{1} - \mathsf{Z}^{\mathrm{C}}\mathsf{Z}^{\mathrm{A_0}})\,|\psi\rangle\,|| = 0,\end{aligned}$$

where the first equality comes from the fact that $(\hat{\mathsf{Z}}^{\dagger})^{\mathrm{A_0}}$ is unitary, the second equality just uses the definition of $\hat{\mathsf{Z}}^{\mathrm{A_0}}$. The third equality is equivalent to $|\mathsf{Z}^{\mathrm{C}}\mathsf{Z}^{\mathrm{A_0}}| = |\mathsf{Z}^{\mathrm{A_0}}|$, which is correct because Z^{C} is unitary. The inequality is a consequence of $A \leq |A|$, and finally the last equality is the consequence of (A.4).

We may now verify equations (8.19) to (8.23) of Lemma 9.5 using the above conditions. The precise isometry that we use is shown in Fig. 8.3. We first verify that the circuit acts correctly on the state $|\psi\rangle^{\mathrm{CA_0}}$. Up to and including the second set of controlled gates the circuit is the well known SWAP circuit, and it is well known (see e.g. [**?**]) that this extracts the maximally entangled state in to the primed auxiliary systems. At this point our state is thus

$$|{+}{+}\rangle^{\mathrm{C''A_0''}}\,\frac{\mathbb{1} + \mathsf{Z}^{\mathrm{C}}}{\sqrt{2}}\,|\psi\rangle^{\mathrm{CA_0}} \otimes |\Phi^{+}\rangle^{\mathrm{C'A_0'}}. \tag{A.10}$$

Let us denote $|\phi\rangle^{\mathrm{CA_0}} = \frac{1}{\sqrt{2}}[\mathbb{1} + \mathsf{Z}^{\mathrm{C}}]\,|\psi\rangle^{\mathrm{CA_0}}$. The third pair of controlled gates evolves the system to

$$\begin{aligned}\frac{1}{2}\Big[\,&|00\rangle^{\mathrm{C''A_0''}}\,|\phi\rangle^{\mathrm{CA_0}} + |01\rangle^{\mathrm{C''A_0''}}\,i\hat{\mathsf{Y}}^{\mathrm{A_0}}\hat{\mathsf{X}}^{\mathrm{A_0}}\,|\phi\rangle^{\mathrm{CA_0}} + \\ &+ |10\rangle^{\mathrm{C''A_0''}}\,i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}}\,|\phi\rangle^{\mathrm{CA_0}} - |11\rangle^{\mathrm{C''A_0''}}\,\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}}\hat{\mathsf{Y}}^{\mathrm{A_0}}\hat{\mathsf{X}}^{\mathrm{A_0}}\,|\phi\rangle^{\mathrm{CA_0}}\Big]\,|\Phi^{+}\rangle^{\mathrm{C'A_0'}}.\end{aligned} \tag{A.11}$$

From (A.7) - (A.9) it follows that $\hat{\mathsf{Y}}^{\mathrm{A_0}}\hat{\mathsf{X}}^{\mathrm{A_0}}\,|\phi\rangle^{\mathrm{CA_0}} = \mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}}\,|\phi\rangle^{\mathrm{CA_0}}$ and so

$$\frac{1}{2}\Big[|00\rangle^{\mathrm{C''A_0''}}\,|\phi\rangle^{\mathrm{CA_0}} + |01\rangle^{\mathrm{C''A_0''}}\,i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}}\,|\phi\rangle^{\mathrm{CA_0}} + |10\rangle^{\mathrm{C''A_0''}}\,i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}}\,|\phi\rangle^{\mathrm{CA_0}} + |11\rangle^{\mathrm{C''A_0''}}\,|\phi\rangle^{\mathrm{CA_0}}\Big]\,|\Phi^{+}\rangle^{\mathrm{C'A_0'}}. \tag{A.12}$$

Finally the last two Hadamards lead to

$$\frac{1}{2\sqrt{2}}\Big[|00\rangle^{\mathrm{C''A_0''}}\,(\mathbb{1} + i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}})(\mathbb{1} + \mathsf{Z}^{\mathrm{C}})\,|\psi\rangle^{\mathrm{CA_0}} + |11\rangle^{\mathrm{C''A_0''}}\,(\mathbb{1} - i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}})(\mathbb{1} + \mathsf{Z}^{\mathrm{C}})\,|\psi\rangle^{\mathrm{CA_0}}\Big]\,|\Phi^{+}\rangle^{\mathrm{C'A_0'}} \tag{A.13}$$

$$= |\xi\rangle^{\mathrm{CC''A_0A_0''}} \otimes |\Phi^{+}\rangle^{\mathrm{C'A_0'}} \tag{A.14}$$

as claimed. Following the same method and using (A.7) - (A.9), one easily verifies

$$U\left(\mathsf{X}^{\mathrm{C}}\,|\psi\rangle^{\mathrm{CA_0}} \otimes |00\rangle\right) = |\xi\rangle^{\mathrm{CC''A_0A_0''}} \otimes \sigma_{\mathrm{X}}^{\mathrm{C'}}\,|\Phi^{+}\rangle^{\mathrm{C'A_0'}}, \quad U\left(\mathsf{Z}^{\mathrm{C}}\,|\psi\rangle^{\mathrm{CA_0}} \otimes |00\rangle\right) = |\xi\rangle^{\mathrm{CC''A_0A_0''}} \otimes \sigma_{\mathrm{Z}}^{\mathrm{C'}}\,|\Phi^{+}\rangle^{\mathrm{C'A_0'}}. \tag{A.15}$$

The case $\mathsf{Y}^{\mathrm{C}}\,|\psi\rangle^{\mathrm{CA}_0}\otimes|00\rangle$ is a bit more involved. After the second pair of controlled gates the state is transformed to

$$|{+}{+}\rangle^{\mathrm{C}''\mathrm{A}_0''}\,\frac{1}{\sqrt{2}}i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}}(\mathbb{1}+\mathsf{Z}^{\mathrm{C}})\,|\psi\rangle^{\mathrm{CA}_0}\,\sigma_{\mathrm{Y}}^{\mathrm{C}'}\,|\Phi^{+}\rangle^{\mathrm{C}'\mathrm{A}_0'}. \tag{A.16}$$

The third pair of controlled gates then transforms the state to

$$\frac{1}{4\sqrt{2}}\Big[|00\rangle^{\mathrm{C}''\mathrm{A}_0''}\,i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}}\,|\phi\rangle^{\mathrm{CA}_0}+|01\rangle^{\mathrm{C}''\mathrm{A}_0''}\,|\phi\rangle^{\mathrm{CA}_0}+|10\rangle^{\mathrm{C}''\mathrm{A}_0''}\,|\phi\rangle^{\mathrm{CA}_0}+|11\rangle^{\mathrm{C}''\mathrm{A}_0''}\,i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}}\,|\phi\rangle^{\mathrm{CA}_0}\Big]\,\sigma_{\mathrm{Y}}^{\mathrm{C}'}\,|\Phi^{+}\rangle^{\mathrm{C}'\mathrm{A}_0'}, \tag{A.17}$$

which is simplified by two last Hadamards to

$$\frac{1}{2\sqrt{2}}\Big[|00\rangle^{\mathrm{C}''\mathrm{A}_0''}\,(\mathbb{1}+i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}})(\mathbb{1}+\mathsf{Z}^{\mathrm{C}})\,|\psi\rangle^{\mathrm{CA}_0}-|11\rangle^{\mathrm{C}''\mathrm{A}_0''}\,(\mathbb{1}-i\mathsf{Y}^{\mathrm{C}}\mathsf{X}^{\mathrm{C}})(\mathbb{1}+\mathsf{Z}^{\mathrm{C}})\,|\psi\rangle^{\mathrm{CA}_0}\Big]\,\sigma_{\mathrm{Y}}^{\mathrm{C}'}\,|\Phi^{+}\rangle^{\mathrm{C}'\mathrm{A}_0'}. \tag{A.18}$$

$$=\sigma_{\mathrm{Z}}^{\mathrm{C}''}\,|\xi\rangle^{\mathrm{CC}''\mathrm{A}_0\mathrm{A}_0''}\otimes\sigma_{\mathrm{Y}}^{C'}\,|\Phi^{+}\rangle^{\mathrm{C}'\mathrm{A}_0'} \tag{A.19}$$

This thus concludes the proof of Lemma 9.5.

Appendix B

Proof of Lemma 9.6

The proof of Lemma 9.6 is split into two parts. The first part proves the necessary self-testing relations between the state and measurements needed to construct the self-testing circuit. The second part verifies that the circuit acts as claimed.

B.1 Self-testing relations

Here we follow closely the proof of [Col17], adapting it the allow for additional σ_{Y} measurements. We first define the following sets of operators:

$$\{\mathsf{Z}_i^{(k)}\}_k = \{\mathsf{O}_{i|\mathbf{z}} | z_i = 1\}; \quad \{\mathsf{X}_i^{(k)}\}_k = \{\mathsf{O}_{i|\mathbf{z}} | z_i = 2\}; \quad \{\mathsf{Y}_i^{(k)}\}_k = \{\mathsf{O}_{i|\mathbf{z}} | z_i = 3\}, \tag{B.1}$$

for $k = 1, \cdots, 3^{n-1}$ and ordered according to some relation $\mathbf{z} < \mathbf{z}'$. Similarly we define

$$\{\mathrm{D}_{\mathrm{xz},i}^{(l)}\}_l = \{\mathrm{P}_{i|\mathbf{x}} | x_i = 1\}; \quad \{\mathrm{E}_{\mathrm{xz},i}^{(l)}\}_l = \{\mathrm{P}_{i|\mathbf{x}} | x_i = 2\}; \quad \{\mathrm{D}_{\mathrm{yz},i}^{(l)}\}_l = \{\mathrm{P}_{i|\mathbf{x}} | x_i = 3\}, \tag{B.2}$$

$$\{\mathrm{E}_{\mathrm{yz},i}^{(l)}\}_l = \{\mathrm{P}_{i|\mathbf{x}} | x_i = 4\}; \quad \{\mathrm{D}_{\mathrm{xy},i}^{(l)}\}_l = \{\mathrm{P}_{i|\mathbf{x}} | x_i = 5\}; \quad \{\mathrm{E}_{\mathrm{xy},i}^{(l)}\}_l = \{\mathrm{P}_{i|\mathbf{x}} | x_i = 6\}. \tag{B.3}$$

for $l = 1, \cdots, 6^{n-1}$ ordered according to some relation $\mathbf{x} < \mathbf{x}'$. Averaging over these sets we thus obtain the operators in equations (8.25) - (8.29). We may now write

$$\begin{aligned}\langle\psi|\mathscr{B}_i|\psi\rangle = &\frac{1}{3^{n-1}6^{n-1}}\sum_{k,l}\langle\psi|\Big[\mathsf{Z}_i^{(k)}(\mathrm{D}_{\mathrm{xz},i}^{(l)} + \mathrm{E}_{\mathrm{xz},i}^{(l)}) + \mathsf{X}_i^{(k)}(\mathrm{D}_{\mathrm{xz},i}^{(l)} - \mathrm{E}_{\mathrm{xz},i}^{(l)}) + \mathsf{Z}_i^{(k)}(\mathrm{D}_{\mathrm{yz},i}^{(l)} + \mathrm{E}_{\mathrm{yz},i}^{(l)}) \\ &- \mathsf{Y}_i^{(k)}(\mathrm{D}_{\mathrm{yz},i}^{(l)} - \mathrm{E}_{\mathrm{yz},i}^{(l)}) + \mathsf{X}_i^{(k)}(\mathrm{D}_{\mathrm{xy},i}^{(l)} + \mathrm{E}_{\mathrm{xy},i}^{(l)}) - \mathsf{Y}_i^{(k)}(\mathrm{D}_{\mathrm{xy},i}^{(l)} - \mathrm{E}_{\mathrm{xy},i}^{(l)})\Big]|\psi\rangle = 6\sqrt{2}\end{aligned} \tag{B.4}$$

for all $i = 1, \cdots, n$. Note that since the maximum value of the triple CHSH inequality is $6\sqrt{2}$ and that the above is a convex mixture of triple CHSH inequalities for different k, l, for each k,l we have

$$\begin{aligned}\langle\psi|\Big[&\mathsf{Z}_i^{(k)}(\mathrm{D}_{\mathrm{xz},i}^{(l)}+\mathrm{E}_{\mathrm{xz},i}^{(l)})+\mathsf{X}_i^{(k)}(\mathrm{D}_{\mathrm{xz},i}^{(l)}-\mathrm{E}_{\mathrm{xz},i}^{(l)})+\mathsf{Z}_i^{(k)}(\mathrm{D}_{\mathrm{yz},i}^{(l)}+\mathrm{E}_{\mathrm{yz},i}^{(l)}) \\ &-\mathsf{Y}_i^{(k)}(\mathrm{D}_{\mathrm{yz},i}^{(l)}-\mathrm{E}_{\mathrm{yz},i}^{(l)})+\mathsf{X}_i^{(k)}(\mathrm{D}_{\mathrm{xy},i}^{(l)}+\mathrm{E}_{\mathrm{xy},i}^{(l)})-\mathsf{Y}_i^{(k)}(\mathrm{D}_{\mathrm{xy},i}^{(l)}-\mathrm{E}_{\mathrm{xy},i}^{(l)})\Big]|\psi\rangle=6\sqrt{2}.\end{aligned} \tag{B.5}$$

Now, we may again use the SOS decomposition (8.12) for each i,k,l leading to

$$\mathsf{Z}_i^{(k)}|\psi\rangle=\frac{\mathrm{D}_{\mathrm{xz},i}^{(l)}+\mathrm{E}_{\mathrm{xz},i}^{(l)}}{\sqrt{2}}|\psi\rangle=\frac{\mathrm{D}_{\mathrm{yz},i}^{(l)}+\mathrm{E}_{\mathrm{yz},i}^{(l)}}{\sqrt{2}}|\psi\rangle, \tag{B.6}$$

$$\mathsf{X}_i^{(k)}|\psi\rangle=\frac{\mathrm{D}_{\mathrm{xz},i}^{(l)}-\mathrm{E}_{\mathrm{xz},i}^{(l)}}{\sqrt{2}}|\psi\rangle=\frac{\mathrm{D}_{\mathrm{xy},i}^{(l)}+\mathrm{E}_{\mathrm{xy},i}^{(l)}}{\sqrt{2}}|\psi\rangle, \tag{B.7}$$

$$\mathsf{Y}_i^{(k)}|\psi\rangle=\frac{\mathrm{D}_{\mathrm{yz},i}^{(l)}-\mathrm{E}_{\mathrm{yz},i}^{(l)}}{\sqrt{2}}|\psi\rangle=\frac{\mathrm{D}_{\mathrm{xy},i}^{(l)}-\mathrm{E}_{\mathrm{xy},i}^{(l)}}{\sqrt{2}}|\psi\rangle, \tag{B.8}$$

which we may write as

$$\mathsf{Z}_i^{(k)}|\psi\rangle=\mathsf{Z}_{i+n}^{(l)}|\psi\rangle;\quad \mathsf{X}_i^{(k)}|\psi\rangle=\mathsf{X}_{i+n}^{(l)}|\psi\rangle;\quad \mathsf{Y}_i^{(k)}|\psi\rangle=\mathsf{Y}_{i+n}^{(l)}|\psi\rangle, \tag{B.9}$$

where

$$\mathsf{Z}_{i+n}^{(l)}=\frac{\mathrm{D}_{\mathrm{xz},i}^{(l)}+\mathrm{E}_{\mathrm{xz},i}^{(l)}}{\sqrt{2}},\quad \mathsf{X}_{i+n}^{(l)}=\frac{\mathrm{D}_{\mathrm{xz},i}^{(l)}-\mathrm{E}_{\mathrm{xz},i}^{(l)}}{\sqrt{2}},\quad \mathsf{Y}_i^{(k)}|\psi\rangle=\frac{\mathrm{D}_{\mathrm{yz},i}^{(l)}-\mathrm{E}_{\mathrm{yz},i}^{(l)}}{\sqrt{2}}. \tag{B.10}$$

As before, equations (B.6) – (B.8) imply mutual anti-communtation of Alice's operators:

$$\{\mathsf{Z}_i^{(k)},\mathsf{X}_i^{(k)}\}=0;\quad \{\mathsf{Z}_i^{(k)},\mathsf{Y}_i^{(k)}\}=0;\quad \{\mathsf{X}_i^{(k)},\mathsf{Y}_i^{(k)}\}=0\quad \forall i,k \tag{B.11}$$

Defining

$$\mathsf{Z}_{i+n}=\frac{1}{6^{n-1}}\sum_l \mathsf{Z}_{i+n}^{(l)};\quad \mathsf{X}_{i+n}=\frac{1}{6^{n-1}}\sum_l \mathsf{X}_{i+n}^{(l)};\quad \mathsf{Y}_{i+n}=-\frac{1}{6^{n-1}}\sum_l \mathsf{Y}_{i+n}^{(l)} \tag{B.12}$$

we have from (B.9)

$$\mathsf{Z}_i^{(k)}|\psi\rangle=\mathsf{Z}_{i+n}|\psi\rangle;\quad \mathsf{X}_i^{(k)}|\psi\rangle=\mathsf{X}_{i+n}|\psi\rangle;\quad \mathsf{Y}_i^{(k)}|\psi\rangle=-\mathsf{Y}_{i+n}|\psi\rangle \tag{B.13}$$

for all k. Note that the operators Z_{i+n}, X_{i+n}, Y_{i+n} are not necessarily unitary. We therefore define the regularized versions of these operators, denoted by $\hat{\mathsf{Z}}_{i+n}$, $\hat{\mathsf{X}}_{i+n}$ and $\hat{\mathsf{Y}}_{i+n}$, which using standard techniques (see for example [BP15, ŠASA16]) can be shown to have the same properties:

$$\mathsf{Z}_i^{(k)}|\psi\rangle=\hat{\mathsf{Z}}_{i+n}|\psi\rangle;\quad \mathsf{X}_i^{(k)}|\psi\rangle=\hat{\mathsf{X}}_{i+n}|\psi\rangle;\quad \mathsf{Y}_i^{(k)}|\psi\rangle=-\hat{\mathsf{Y}}_{i+n}|\psi\rangle. \tag{B.14}$$

At this point we are nearly ready to construct our self-testing unitary. However, we still need to prove that $P_i^{(k)}$ and $P_j^{(k)}$ for $P \in \{\mathsf{X},\mathsf{Y},\mathsf{Z}\}$ commute for $i \neq j$. Here, we again use the method of [Col17] to achieve this, which we restate here. Note that for every $i \neq j$, if we fix $z_i = 1$ and $z_j = 1$, there are 3^{n-2} choices for Charlie's measurement vector $\mathbf{z}$. There are thus 3^{n-2} pairs of indices (k,k') such that operators $\mathsf{Z}_i^{(k)}$ and $\mathsf{Z}_i^{(k')}$ are built from the same set of orthogonal projectors that commute by construction. We thus have 3^{n-2} equations of the form

$$\mathsf{Z}_i^{(k)}\mathsf{Z}_j^{(k')}|\psi\rangle = \mathsf{Z}_j^{(k')}\mathsf{Z}_i^{(k)}|\psi\rangle\,. \tag{B.15}$$

Choosing a pair (k,k') and using (B.13) and the fact that operators on Chalie and Alice's subsystems commute we then obtain

$$\mathsf{Z}_i^{(k)}\mathsf{Z}_{n+j}|\psi\rangle = \mathsf{Z}_j^{(k')}\mathsf{Z}_{n+i}|\psi\rangle \tag{B.16}$$

$$\mathsf{Z}_{n+j}\mathsf{Z}_i^{(k)}|\psi\rangle = \mathsf{Z}_{n+i}\mathsf{Z}_j^{(k')}|\psi\rangle \tag{B.17}$$

$$\mathsf{Z}_{n+j}\mathsf{Z}_{n+i}|\psi\rangle = \mathsf{Z}_{n+i}\mathsf{Z}_{n+j}|\psi\rangle\,. \tag{B.18}$$

In fact, by working backwards using different values of k, k' and (B.13) again, one sees

$$\mathsf{Z}_i^{(k)}\mathsf{Z}_j^{(k')}|\psi\rangle = \mathsf{Z}_j^{(k')}\mathsf{Z}_i^{(k)}|\psi\rangle \qquad \forall k,k',i \neq j. \tag{B.19}$$

In the same fashion, one proves

$$\mathsf{X}_i^{(k)}\mathsf{X}_j^{(k')}|\psi\rangle = \mathsf{X}_j^{(k')}\mathsf{X}_i^{(k)}|\psi\rangle \qquad \forall k,k',i \neq j, \tag{B.20}$$

$$\mathsf{Y}_i^{(k)}\mathsf{Y}_j^{(k')}|\psi\rangle = \mathsf{Y}_j^{(k')}\mathsf{Y}_i^{(k)}|\psi\rangle \qquad \forall k,k',i \neq j, \tag{B.21}$$

$$\mathsf{X}_i^{(k)}\mathsf{Y}_j^{(k')}|\psi\rangle = \mathsf{Y}_j^{(k')}\mathsf{X}_i^{(k)}|\psi\rangle \qquad \forall k,k',i \neq j, \tag{B.22}$$

$$\mathsf{X}_i^{(k)}\mathsf{Z}_j^{(k')}|\psi\rangle = \mathsf{Z}_j^{(k')}\mathsf{X}_i^{(k)}|\psi\rangle \qquad \forall k,k',i \neq j, \tag{B.23}$$

$$\mathsf{Y}_i^{(k)}\mathsf{Z}_j^{(k')}|\psi\rangle = \mathsf{Z}_j^{(k')}\mathsf{Y}_i^{(k)}|\psi\rangle \qquad \forall k,k',i \neq j, \tag{B.24}$$

We have now finished the necessary groundwork to construct the self-testing circuit of Lemma 9.6.

B.2 Verification of circuit

The circuit we use (see Fig. B.1) is a parallel version of the circuit used in the two qubit case. To prove that it functions correctly, we make repeated use of the properties (B.11), (B.14) and (B.19) - (B.24). Before the action of the first controlled gate the system is in state

$$|\psi\rangle^{\mathrm{CA}_0}\frac{1}{2^{2n}}\sum_{p,q,r,s\in(0,1)^n}|p\rangle^{\mathrm{C}'}|q\rangle^{\mathrm{C}''}|r\rangle^{\mathrm{A}_0'}|s\rangle^{\mathrm{A}_0''}, \tag{B.25}$$

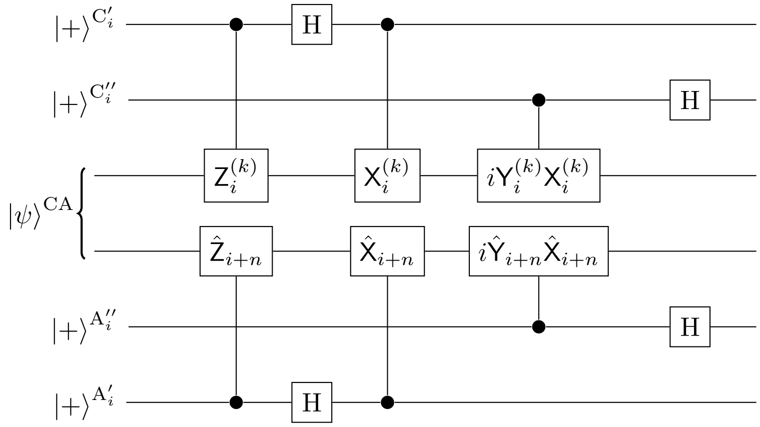
$|+\rangle^{\mathrm{C}'_i}$
$|+\rangle^{\mathrm{C}''_i}$
$|\psi\rangle^{\mathrm{CA}}$
$|+\rangle^{\mathrm{A}''_i}$
$|+\rangle^{\mathrm{A}'_i}$
H
H
H
H
$\mathsf{Z}_i^{(k)}$
$\mathsf{X}_i^{(k)}$
$i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)}$
$\hat{\mathsf{Z}}_{i+n}$
$\hat{\mathsf{X}}_{i+n}$
$i\hat{\mathsf{Y}}_{i+n}\hat{\mathsf{X}}_{i+n}$

Figure B.1: Circuit diagram representing the local unitary of Lemma 2. The total unitary consists of applying this circuit for each $i = 1,\cdots,n$, and k can be chosen to be any number $k = 1,\cdots,3^{n-1}$ (for example $k = 1$).

and after the first controlled gate the state evolves to

$$\frac{1}{2^{2n}}\sum_{p,q,r,s\in(0,1)^n}\left[\otimes_{i=1}^{n}(\mathsf{Z}_i^{(k)})^{p_i}(\hat{\mathsf{Z}}_{i+n})^{r_i}\,|\psi\rangle^{\mathrm{CA}_0}\right]|p\rangle^{\mathrm{C}'}|q\rangle^{\mathrm{C}''}|r\rangle^{\mathrm{A}'_0}|s\rangle^{\mathrm{A}''_0}, \tag{B.26}$$

where $p_i(r_i)$ is the i-th element of string $p(r)$. Hadamard gates evolve the state to

$$\frac{1}{2^{3n}}\sum_{p,q,r,s\in(0,1)^n}\left[\otimes_{i=1}^{n}(\mathbb{1}+(-1)^{p_i}\mathsf{Z}_i^{(k)})(\mathbb{1}+(-1)^{r_i}\hat{\mathsf{Z}}_{i+n})\,|\psi\rangle^{\mathrm{CA}_0}\right]|p\rangle^{\mathrm{C}'}|q\rangle^{\mathrm{C}''}|r\rangle^{\mathrm{A}'_0}|s\rangle^{\mathrm{A}''_0}, \tag{B.27}$$

and the second controlled gates lead to

$$\frac{1}{2^{3n}}\sum_{p,q,r,s\in(0,1)^n}\left[\otimes_{i=1}^{n}(\mathsf{X}_i^{(k)})^{p_i}(\mathbb{1}+(-1)^{p_i}\mathsf{Z}_i^{(k)})(\hat{\mathsf{X}}_{n+i})^{r_i}(\mathbb{1}+(-1)^{r_i}\hat{\mathsf{Z}}_{i+n})\,|\psi\rangle^{\mathrm{CA}_0}\right]|p\rangle^{\mathrm{C}'}|q\rangle^{\mathrm{C}''}|r\rangle^{\mathrm{A}'_0}|s\rangle^{\mathrm{A}''_0}. \tag{B.28}$$

Relations (B.14) and (B.23) allow us to simplify this to

$$\frac{1}{2^{3n}}\sum_{p,q,r,s\in(0,1)^n}\left[\otimes_{i=1}^{n}(\mathsf{X}_i^{(k)})^{p_i}(\mathbb{1}+(-1)^{p_i}\mathsf{Z}_i^{(k)})(\hat{\mathsf{X}}_{n+i})^{r_i}(\mathbb{1}+(-1)^{r_i}\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA}_0}\right]|p\rangle^{\mathrm{C}'}|q\rangle^{\mathrm{C}''}|r\rangle^{\mathrm{A}'_0}|s\rangle^{\mathrm{A}''_0}. \tag{B.29}$$

Unitarity and hermiticity of $\mathsf{Z}_i^{(k)}$ implies $(\mathbb{1}+\mathsf{Z}_i^{(k)})(\mathbb{1}-\mathsf{Z}_i^{(k)})\,|\psi\rangle = 0$ and $\frac{1}{4}(\mathbb{1}+\mathsf{Z}_i^{(k)})(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle = \frac{1}{2}(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle$ so that for every i the state of the system can be further simplified to obtain

$$\frac{1}{2^{2n}}\sum_{p,q,s\in(0,1)^n}\left[\otimes_{i=1}^{n}(\mathsf{X}_i^{(k)})^{p_i}(\mathbb{1}+(-1)^{p_i}\mathsf{Z}_i^{(k)})(\hat{\mathsf{X}}_{n+i})^{p_i}\,|\psi\rangle^{\mathrm{CA}_0}\right]|p\rangle^{\mathrm{C}'}|q\rangle^{\mathrm{C}''}|p\rangle^{\mathrm{A}'_0}|s\rangle^{\mathrm{A}''_0}. \tag{B.30}$$

This can be further simplified by using (B.11) and (B.20):

$$\frac{1}{2^{2n}} \sum_{p,q,s\in(0,1)^n} \left[\otimes_{i=1}^{n}(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA}_0}\right] |p\rangle^{\mathrm{C}'} |q\rangle^{\mathrm{C}''} |p\rangle^{\mathrm{A}_0'} |s\rangle^{\mathrm{A}_0''}$$
$$= \frac{1}{2^{\frac{3n}{2}}} \sum_{q,s\in(0,1)^n} \left[\otimes_{i=1}^{n}(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA}_0}\right] \left[\otimes_{i=1}^{n}|\Phi^{+}\rangle^{\mathrm{C}_i'\mathrm{A}_i'}\right] |q\rangle^{\mathrm{C}''} |s\rangle^{\mathrm{A}_0''}. \quad \text{(B.31)}$$

Already here the state of the primed auxiliarys (extraction auxiliarys in the following text) is n-fold tensor product of maximally entangled pairs of qubits. Since the rest of the circuit does not affect extraction auxiliarys for the sake of simplicity it will be omitted from the following expressions. Following the action of the third pair of controlled gates the system evolves to

$$\frac{1}{2^{\frac{3n}{2}}} \sum_{q,s\in(0,1)^n} \left[\otimes_{i=1}^{n}(i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})^{q_i}(\mathbb{1}+\mathsf{Z}_i^{(k)})(i\hat{\mathsf{Y}}_{n+i}\hat{\mathsf{X}}_{n+i})^{s_i}\,|\psi\rangle^{\mathrm{CA}_0}\right] |q\rangle^{\mathrm{C}''} |s\rangle^{\mathrm{A}_0''}, \quad \text{(B.32)}$$

By virtue of (B.14), (B.11), (B.24), (B.22) and (B.23) this simplifies to

$$\frac{1}{2^{\frac{3n}{2}}} \sum_{q,s\in(0,1)^n} \left[\otimes_{i=1}^{n}(i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})^{q_i+s_i}(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA}_0}\right] |q\rangle^{\mathrm{C}''} |s\rangle^{\mathrm{A}_0''}, \quad \text{(B.33)}$$

Finally at the end of the circuit, after the action of the second pair of Hadamards we have:

$$\frac{1}{2^{\frac{5n}{2}}} \sum_{q,s,\bar{q},\bar{s}\in(0,1)^n} \left[\otimes_{i=1}^{n}(-1)^{\bar{q}_i q_i+\bar{s}_i s_i}(i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})^{q_i+s_i}(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA}_0}\right] |\bar{q}\rangle^{\mathrm{C}''} |\bar{s}\rangle^{\mathrm{A}_0''}. \quad \text{(B.34)}$$

Note that each term from the sum is characterized by a pair of strings $(\bar{q},\bar{s})$ and a set of pairs of strings Ξ, such that $q_j''+s_j''=q_j'+s_j'$ for every $q'',s'',q',s'\in\Xi$ and every j. We show that the multiplicative factor in front of every term is equal to zero whenever $\bar{q}'\neq\bar{s}'$. Let us assume $\bar{q}'=\bar{s}'$. The multiplicative factor for a term corresponding to a pair of strings q',s' is equal to

$$(-1)^{\sum_{q',s'\in\Xi,j}\bar{q}_j'q_j'+\bar{s}_j's_j'} = (-1)^{\sum_{q',s'\in\Xi,j}\bar{q}_j'(q_j'+s_j')} = \pm 1,$$

i.e., all the terms come with the same sign, since sum is over q',s' which have fixed $q_j'+s_j'$ for every j. Contrarily, in case $\bar{q}'\neq\bar{s}'$ the multiplicative factor for a term corresponding to a pair of strings q',s' is equal to

$$(-1)^{\sum_{q',s'\in\Xi,j}\bar{q}_j'q_j'+\bar{s}_j's_j'} = (-1)^{\sum_{q',s'\in\Xi,j}\bar{q}_j'(q_j'+s_j')+(\bar{s}_j'-\bar{q}_j')s_j'} = \begin{cases}\pm 1 & \text{when} \quad \sum_j s_j'=0\\ \mp 1 & \text{when} \quad \sum_j s_j'=1\end{cases}$$
$$= 0.$$

In this case value of s'_j determines the sign of the terms, and for half of the terms it is equal 0 (one sign) and for the half it is equal to 1 (opposite sign). This means that only terms of the sum which survive are those corresponding to $\bar{q} = \bar{s}$.

$$\frac{1}{2^{\frac{5n}{2}}} \sum_{q,s,\bar{q}\in(0,1)^n} \left[\otimes_{i=1}^n (-1)^{\bar{q}_i(q_i+s_i)} (i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})^{q_i+s_i} (\mathbb{1} + \mathsf{Z}_i^{(k)}) \left|\psi\right\rangle^{\mathrm{CA}_0}\right] \left|\bar{q}\bar{q}\right\rangle^{\mathrm{C''A''_0}}. \tag{B.35}$$

The sum has 2^{3n} different contributions (one for each triple $q,s,\bar{q}$), but there are 2^{2n} different terms, meaning that each term has contributions from 2^n different pairs of strings (q,s). This reduces the multiplicative factor in front of the sum to $2^{-\frac{3n}{2}}$. After summing over q,s and making some rearrangements the expression reduces to

$$\left|\xi\right\rangle = \frac{1}{2^{\frac{3n}{2}}} \sum_{\bar{q}\in(0,1)^n} \left[\otimes_{i=1}^n (\mathbb{1} + (-1)^{\bar{q}_i} i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})(\mathbb{1} + \mathsf{Z}_i^{(k)}) \left|\psi\right\rangle^{\mathrm{CA}_0}\right] \left|\bar{q}\bar{q}\right\rangle^{\mathrm{C''A''_0}}. \tag{B.36}$$

Finally, by returning the state of extraction auxiliary systems one obtains the statement from Lemma 2:

$$U\left[\left|\psi\right\rangle^{\mathrm{CA}} \otimes \left|00\right\rangle\right] = \left|\xi\right\rangle \otimes_{i=1}^n \left|\Phi^+\right\rangle^{\mathrm{C'_iA'_i}}. \tag{B.37}$$

Before calculating the output of the circuit when the input is $\mathsf{Z}_i^{(k)}\left|\psi\right\rangle$ let us acknowledge that $\mathsf{Z}_i^{(k)}\left|\psi\right\rangle = \mathsf{Z}_i^{(l)}\left|\psi\right\rangle$ for any two l and k, which can be seen from (B.14) which is satisfied for any k. The same holds for $\mathsf{X}_i^{(k)}\left|\psi\right\rangle$ and $\mathsf{Y}_i^{(k)}\left|\psi\right\rangle$. By repeating the same procedure as in the derivation above one can confirm two more statements from Lemma 2 for any k and j:

$$\begin{aligned} U\left[\mathsf{Z}_j^{(k)}\left|\psi\right\rangle^{\mathrm{CA}_0} \otimes \left|00\right\rangle\right] &= \left|\xi\right\rangle \left[\sigma_{\mathrm{Z}}{}^{\mathrm{C'_j}} \otimes_{i=1}^n \left|\Phi^+\right\rangle^{\mathrm{C'_iA'_i}}\right], \\ U\left[\mathsf{X}_j^{(k)}\left|\psi\right\rangle^{\mathrm{CA}_0} \otimes \left|00\right\rangle\right] &= \left|\xi\right\rangle \left[\sigma_{\mathrm{X}}{}^{\mathrm{C'_j}} \otimes_{i=1}^n \left|\Phi^+\right\rangle^{\mathrm{C'_iA'_i}}\right]. \end{aligned} \tag{B.38}$$

The situation when the input state is $\mathsf{Y}_j^{(k)}\left|\psi\right\rangle$ is a bit more complicated so more details of the derivation will be presented. After the second pair of controlled gates the state of the system is:

$$\frac{1}{2^{3n}} \sum_{p,q,r,s\in(0,1)^n} \left[\otimes_{i=1}^n (\mathsf{X}_i^{(k)})^{p_i} (\mathbb{1} + (-1)^{p_i}\mathsf{Z}_i^{(k)}) \mathsf{Y}_j^{(k)} (\hat{\mathsf{X}}_{n+i})^{r_i} (\mathbb{1} + (-1)^{r_i}\hat{\mathsf{Z}}_{i+n}) \left|\psi\right\rangle^{\mathrm{CA}_0}\right] \left|p\right\rangle^{\mathrm{C'}} \left|q\right\rangle^{\mathrm{C''}} \left|r\right\rangle^{\mathrm{A'_0}} \left|s\right\rangle^{\mathrm{A''_0}}, \tag{B.39}$$

which due to eqs. (B.11) and (B.24) simplifies to

$$\frac{1}{2^{3n}} \sum_{p,q,r,s\in(0,1)^n} \left[\otimes_{i=1}^n (\mathsf{X}_i^{(k)})^{p_i} \mathsf{Y}_j^{(k)} (\mathbb{1} + (-1)^{p_i\oplus\delta_{ij}}\mathsf{Z}_i^{(k)}) (\hat{\mathsf{X}}_{n+i})^{r_i} (\mathbb{1} + (-1)^{r_i}\hat{\mathsf{Z}}_{i+n}) \left|\psi\right\rangle^{\mathrm{CA}_0}\right] \left|pq\right\rangle^{\mathrm{C'C''}} \left|rs\right\rangle^{\mathrm{A'_0A''_0}}, \tag{B.40}$$

By using (B.19), (B.11) and the fact that $\frac{\mathbb{1}+\mathsf{Z}_i^{(k)}}{2}$ and $\frac{\mathbb{1}-\mathsf{Z}_i^{(k)}}{2}$ are projectors onto different eigenspaces of $\mathsf{Z}_i^{(k)}$ the above reduces to

$$\frac{1}{2^{2n}} \sum_{q,r,s\in(0,1)^n} \left[\otimes_{i=1}^n (-1)^{r_i\oplus\delta_{ij}} \mathsf{Y}_j^{(k)}\mathsf{X}_j^{(k)}(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA_0}}\right] |r\oplus 1_j\rangle^{\mathrm{C'}} |q\rangle^{\mathrm{C''}} |r\rangle^{\mathrm{A'_0}} |s\rangle^{\mathrm{A''_0}}, \tag{B.41}$$

where 1_j is an n-element string whose j-th element is one with all the other elements being zeros. The last expression can be rewritten in the following way:

$$\frac{1}{2^{\frac{3n}{2}}} \sum_{q,s\in(0,1)^n} \left[\otimes_{i=1}^n i\mathsf{Y}_j^{(k)}\mathsf{X}_j^{(k)}(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA}}\right] \sigma_{\mathrm{Y}}^{\mathrm{C'_j}} \left[\otimes_{i=1}^n |\Phi^+\rangle^{\mathrm{C'_iA'_i}}\right] |q\rangle^{\mathrm{C''}} |s\rangle^{\mathrm{A''_0}}. \tag{B.42}$$

Since the rest of the circuit does not affect the state of extraction auxiliarys we will drop it from the following few equations. After applying the third pair of controlled gates on this state one obtains

$$\frac{1}{2^{\frac{3n}{2}}} \sum_{q,s\in(0,1)^n} \left[\otimes_{i=1}^n (i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})^{q_i+\delta_{ij}}(\mathbb{1}+\mathsf{Z}_i^{(k)})(i\hat{\mathsf{Y}}_{i+n}\hat{\mathsf{X}}_{i+n})^{s_i}\,|\psi\rangle^{\mathrm{CA_0}}\right] |q\rangle^{\mathrm{C''}} |s\rangle^{\mathrm{A''_0}}, \tag{B.43}$$

which due to (B.14) and anticommuting relations (B.11) reduces to:

$$\frac{1}{2^{\frac{3n}{2}}} \sum_{q,s\in(0,1)^n} \left[\otimes_{i=1}^n (i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})^{s_i+q_i+\delta_{ij}}(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA_0}}\right] |q\rangle^{\mathrm{C''}} |s\rangle^{\mathrm{A''_0}}, \tag{B.44}$$

and at the end of the circuit following the action of two last Hadamards this state transforms to

$$\frac{1}{2^{\frac{5n}{2}}} \sum_{\bar{q},\bar{s},q,s\in(0,1)^n} (-1)^{\bar{q}_iq_i+\bar{s}_is_i} \left[\otimes_{i=1}^n (i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})^{q_i+s_i+\delta_{ij}}(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA_0}}\right] |\bar{q}\rangle^{\mathrm{C''}} |s\rangle^{\mathrm{A''_0}}. \tag{B.45}$$

Here the same reasoning like the one preceding to eq. (B.36) can be applied, the only difference being factor $(i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})^{\delta_{ij}}$. This factor changes the sign of terms in (B.36) which correspond to any string $\bar{q}$ for which $\bar{q}_j = 1$. The final form of the output of the circuit when input is $\mathsf{Y}_j^{(k)}\,|\psi\rangle$ can be written as

$$\frac{1}{2^{\frac{3n}{2}}} \sum_{\bar{q}\in(0,1)^n} \left[\otimes_{i=1}^n (-1)^{\bar{q}_j}(\mathbb{1}+(-1)^{\bar{q}_i} i\mathsf{Y}_i^{(k)}\mathsf{X}_i^{(k)})(\mathbb{1}+\mathsf{Z}_i^{(k)})\,|\psi\rangle^{\mathrm{CA_0}}\right] \sigma_{\mathrm{Y}}^{\mathrm{C'_j}} \left[\otimes_{i=1}^n |\Phi^+\rangle^{\mathrm{C'_iA'_i}}\right] |\bar{q}\bar{q}\rangle^{\mathrm{C''A''_0}}, \tag{B.46}$$

which is equivalent to the formulation from Lemma 2:

$$U\left[\mathsf{Y}_j^{\mathrm{C}}\,|\psi\rangle^{\mathrm{CA_0}}\otimes|00\rangle\right] = \sigma_{\mathrm{Z}}{}^{\mathrm{C''_j}}\,|\xi\rangle \left[\sigma_{\mathrm{Y}}{}^{\mathrm{C'_j}}\otimes_{i=1}^n |\Phi^+\rangle^{\mathrm{C'_iA'_i}}\right] \tag{B.47}$$

which completes the proof.

Appendix C

Proof of Lemma 9.7

Correlations $\langle\psi|\mathsf{S}_{l,a}|\psi\rangle = \langle\psi|\mathsf{S}_{l,a}|\psi\rangle = \frac{1}{4}$ for every $l \in \{1,\dots m\}$ and $a \in \{0,1,2,3\}$, given in Table 8.1, imply that the norm of states $\mathsf{S}_{l,a}|\psi\rangle$ and $\mathsf{T}_{l,a}|\psi\rangle$ is equal to $\frac{1}{2}$. These correlations allow us to write

$$\mathsf{S}_{l,0}|\psi\rangle \sim \frac{1}{4}\Big(|\psi\rangle + \mathsf{Z}^{(k)}_{2l-1}\mathsf{Z}^{(k)}_{2l}|\psi\rangle + \mathsf{X}^{(k)}_{2l-1}\mathsf{X}^{(k)}_{2l}|\psi\rangle - \mathsf{Y}^{(k)}_{2l-1}\mathsf{Y}^{(k)}_{2l}|\psi\rangle\Big). \tag{C.1}$$

Since states $|\psi\rangle$, $\mathsf{Z}^{(k)}_{2l-1}\mathsf{Z}^{(k)}_{2l}|\psi\rangle$, $\mathsf{X}^{(k)}_{2l-1}\mathsf{X}^{(k)}_{2l}|\psi\rangle$ and $\mathsf{Y}^{(k)}_{2l-1}\mathsf{Y}^{(k)}_{2l}|\psi\rangle$ all have unit norm and are mutually orthogonal they can be seen as a part of basis of all states from $\mathscr{H}^{\mathrm{C}} \otimes \mathscr{H}^{\mathrm{A}_0}$. Moreover $\mathsf{S}_{l,0}|\psi\rangle$ has the same norm as the expression from the right hand side of $\sim$ in eq. (C.1) which implies that

$$\mathsf{S}_{l,0}|\psi\rangle = \frac{1}{4}\Big(|\psi\rangle + \mathsf{Z}^{(k)}_{2l-1}\mathsf{Z}^{(k)}_{2l}|\psi\rangle + \mathsf{X}^{(k)}_{2l-1}\mathsf{X}^{(k)}_{2l}|\psi\rangle - \mathsf{Y}^{(k)}_{2l-1}\mathsf{Y}^{(k)}_{2l}|\psi\rangle\Big). \tag{C.2}$$

The same reasoning leads to the following set of equations:

$$\mathsf{S}_{l,1}|\psi\rangle = \frac{1}{4}\Big(|\psi\rangle + \mathsf{Z}^{(k)}_{2l-1}\mathsf{Z}^{(k)}_{2l}|\psi\rangle - \mathsf{X}^{(k)}_{2l-1}\mathsf{X}^{(k)}_{2l}|\psi\rangle + \mathsf{Y}^{(k)}_{2l-1}\mathsf{Y}^{(k)}_{2l}|\psi\rangle\Big), \tag{C.3}$$

$$\mathsf{S}_{l,2}|\psi\rangle = \frac{1}{4}\Big(|\psi\rangle - \mathsf{Z}^{(k)}_{2l-1}\mathsf{Z}^{(k)}_{2l}|\psi\rangle + \mathsf{X}^{(k)}_{2l-1}\mathsf{X}^{(k)}_{2l}|\psi\rangle + \mathsf{Y}^{(k)}_{2l-1}\mathsf{Y}^{(k)}_{2l}|\psi\rangle\Big), \tag{C.4}$$

$$\mathsf{S}_{l,3}|\psi\rangle = \frac{1}{4}\Big(|\psi\rangle - \mathsf{Z}^{(k)}_{2l-1}\mathsf{Z}^{(k)}_{2l}|\psi\rangle - \mathsf{X}^{(k)}_{2l-1}\mathsf{X}^{(k)}_{2l}|\psi\rangle - \mathsf{Y}^{(k)}_{2l-1}\mathsf{Y}^{(k)}_{2l}|\psi\rangle\Big), \tag{C.5}$$

$$\mathsf{T}_{l,0}|\psi\rangle = \frac{1}{4}\Big(|\psi\rangle + \mathsf{Z}^{(k)}_{2l}\mathsf{Z}^{(k)}_{2l+1}|\psi\rangle + \mathsf{X}^{(k)}_{2l}\mathsf{X}^{(k)}_{2l+1}|\psi\rangle - \mathsf{Y}^{(k)}_{2l}\mathsf{Y}^{(k)}_{2l+1}|\psi\rangle\Big), \tag{C.6}$$

$$\mathsf{T}_{l,1}|\psi\rangle = \frac{1}{4}\Big(|\psi\rangle + \mathsf{Z}^{(k)}_{2l}\mathsf{Z}^{(k)}_{2l+1}|\psi\rangle - \mathsf{X}^{(k)}_{2l}\mathsf{X}^{(k)}_{2l+1}|\psi\rangle + \mathsf{Y}^{(k)}_{2l}\mathsf{Y}^{(k)}_{2l+1}|\psi\rangle\Big), \tag{C.7}$$

$$\mathsf{T}_{l,2}|\psi\rangle = \frac{1}{4}\Big(|\psi\rangle - \mathsf{Z}^{(k)}_{2l}\mathsf{Z}^{(k)}_{2l+1}|\psi\rangle + \mathsf{X}^{(k)}_{2l}\mathsf{X}^{(k)}_{2l+1}|\psi\rangle + \mathsf{Y}^{(k)}_{2l}\mathsf{Y}^{(k)}_{2l+1}|\psi\rangle\Big), \tag{C.8}$$

$$\mathsf{T}_{l,3}|\psi\rangle = \frac{1}{4}\Big(|\psi\rangle - \mathsf{Z}^{(k)}_{2l}\mathsf{Z}^{(k)}_{2l+1}|\psi\rangle - \mathsf{X}^{(k)}_{2l}\mathsf{X}^{(k)}_{2l+1}|\psi\rangle - \mathsf{Y}^{(k)}_{2l}\mathsf{Y}^{(k)}_{2l+1}|\psi\rangle\Big). \tag{C.9}$$

Equations (C.2-C.5) are equivalent to the following set of equations

$$\begin{aligned}
\mathsf{Z}^{(k)}_{2l-1}\mathsf{Z}^{(k)}_{2l}\left|\psi\right\rangle &= \left(\mathsf{S}_{l,0}+\mathsf{S}_{l,1}-\mathsf{S}_{l,2}-\mathsf{S}_{l,3}\right)\left|\psi\right\rangle, && \text{(C.10a)}\\
\mathsf{X}^{(k)}_{2l-1}\mathsf{X}^{(k)}_{2l}\left|\psi\right\rangle &= \left(\mathsf{S}_{l,0}-\mathsf{S}_{l,1}+\mathsf{S}_{l,2}-\mathsf{S}_{l,3}\right)\left|\psi\right\rangle, && \text{(C.10b)}\\
\mathsf{Y}^{(k)}_{2l-1}\mathsf{Y}^{(k)}_{2l}\left|\psi\right\rangle &= \left(-\mathsf{S}_{l,0}+\mathsf{S}_{l,1}+\mathsf{S}_{l,2}-\mathsf{S}_{l,3}\right)\left|\psi\right\rangle. && \text{(C.10c)}
\end{aligned}$$

Based on the last set of equations and the fact that $\{\mathsf{S}_{l,a}\}_{l,a}$ is orthogonal set of projectors which all commute with all the operators from $\{\mathsf{Z}^{(k)}_j,\mathsf{X}^{(k)}_j\}_{j,k}$ one can show that

$$\begin{aligned}
\mathsf{X}^{(k)}_{2l-1}\mathsf{X}^{(k)}_{2l}\mathsf{Z}^{(k)}_{2l-1}\mathsf{Z}^{(k)}_{2l}\left|\psi\right\rangle &= \mathsf{X}^{(k)}_{2l-1}\mathsf{X}^{(k)}_{2l}\left(\mathsf{S}_{l,0}+\mathsf{S}_{l,1}-\mathsf{S}_{l,2}-\mathsf{S}_{l,3}\right)\left|\psi\right\rangle\\
&= \left(\mathsf{S}_{l,0}+\mathsf{S}_{l,1}-\mathsf{S}_{l,2}-\mathsf{S}_{l,3}\right)\left(\mathsf{S}_{l,0}-\mathsf{S}_{l,1}+\mathsf{S}_{l,2}-\mathsf{S}_{l,3}\right)\left|\psi\right\rangle\\
&= \left(\mathsf{S}_{l,0}-\mathsf{S}_{l,1}-\mathsf{S}_{l,2}+\mathsf{S}_{l,3}\right)\left|\psi\right\rangle\\
&= -\mathsf{Y}^{(k)}_{2l-1}\mathsf{Y}^{(k)}_{2l}\left|\psi\right\rangle. \qquad \text{(C.11)}
\end{aligned}$$

Starting from equations (C.6-C.9) one can obtain

$$\mathsf{X}^{(k)}_{2l}\mathsf{X}^{(k)}_{2l+1}\mathsf{Z}^{(k)}_{2l}\mathsf{Z}^{(k)}_{2l+1}\left|\psi\right\rangle = -\mathsf{Y}^{(k)}_{2l}\mathsf{Y}^{(k)}_{2l+1}\left|\psi\right\rangle. \qquad \text{(C.12)}$$

Equations (C.11) and (C.12) hold for every k and every l. Let us take $l=1$ and check how eq. (C.11) affects vector $\left|\xi_{\bar{q}}\right\rangle = \otimes_{i=1}^{n}(\mathbb{1}+(-1)^{\bar{q}_i}i\mathsf{Y}^{(k)}_i\mathsf{X}^{(k)}_i)(\mathbb{1}+\mathsf{Z}^{(k)}_i)\left|\psi\right\rangle$. Let us write it in the following form:

$$\left|\xi_{\bar{q}}\right\rangle = L_{\text{rest}}\otimes\left(\mathbb{1}+(-1)^{\bar{q}_1}i\mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\right)\left(\mathbb{1}+\mathsf{Z}^{(k)}_1\right)\otimes\left(\mathbb{1}+(-1)^{\bar{q}_2}i\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\right)\left(\mathbb{1}+\mathsf{Z}^{(k)}_2\right)\left|\psi\right\rangle$$

where $L_{\text{rest}} = \otimes_{i=3}^{n}(\mathbb{1}+(-1)^{\bar{q}_i}i\mathsf{Y}^{(k)}_i\mathsf{X}^{(k)}_i)(\mathbb{1}+\mathsf{Z}^{(k)}_i)$. Let us assume $\bar{q}_1\neq\bar{q}_2$ and omit L_{rest} for the sake of shorter exposition. Then $\left|\xi_{\bar{q}}\right\rangle$ reads

$$\begin{aligned}
&\left|\psi\right\rangle \pm i\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\left|\psi\right\rangle + \mathsf{Z}^{(k)}_2\left|\psi\right\rangle \pm i\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\mathsf{Z}^{(k)}_2\left|\psi\right\rangle \mp i\mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\left|\psi\right\rangle + \mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\left|\psi\right\rangle \mp\\
&\mp i\mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_2\left|\psi\right\rangle + \mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\mathsf{Z}^{(k)}_2\left|\psi\right\rangle + \mathsf{Z}^{(k)}_1\left|\psi\right\rangle \pm i\mathsf{Z}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\left|\psi\right\rangle + \mathsf{Z}^{(k)}_1\mathsf{Z}^{(k)}_2\left|\psi\right\rangle \pm\\
&\pm i\mathsf{Z}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\mathsf{Z}^{(k)}_2\left|\psi\right\rangle \mp i\mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_1\left|\psi\right\rangle + \mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\left|\psi\right\rangle \mp i\mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_1\mathsf{Z}^{(k)}_2\left|\psi\right\rangle +\\
&+\mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\mathsf{Z}^{(k)}_2\left|\psi\right\rangle.
\end{aligned}$$

This expression can be written as a sum of expressions, each equal to 0. To show this let us rearrange eq. (C.11) for the case $l=1$. It can be written in eight different ways, which are given below.

$$\begin{aligned}
&\left|\psi\right\rangle + \mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\mathsf{Z}^{(k)}_2\left|\psi\right\rangle = 0, \qquad && \mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\left|\psi\right\rangle + \mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_1\mathsf{Z}^{(k)}_2\left|\psi\right\rangle = 0,\\
&\mathsf{Z}^{(k)}_2\left|\psi\right\rangle + \mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\left|\psi\right\rangle = 0, && \mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\mathsf{Z}^{(k)}_2\left|\psi\right\rangle + \mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_1\left|\psi\right\rangle = 0,\\
&\mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\left|\psi\right\rangle + \mathsf{Z}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\mathsf{Z}^{(k)}_2\left|\psi\right\rangle = 0, && \mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\left|\psi\right\rangle + \mathsf{Z}^{(k)}_1\mathsf{Z}^{(k)}_2\left|\psi\right\rangle = 0,\\
&\mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Z}^{(k)}_2\left|\psi\right\rangle + \mathsf{Z}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\left|\psi\right\rangle = 0, && \mathsf{Y}^{(k)}_1\mathsf{X}^{(k)}_1\mathsf{Y}^{(k)}_2\mathsf{X}^{(k)}_2\mathsf{Z}^{(k)}_2\left|\psi\right\rangle + \mathsf{Z}^{(k)}_1\left|\psi\right\rangle = 0.
\end{aligned}$$

(C.13)

All these equations are obtained from eq. (C.11) by using commutation relations (B.19), expressions (B.14), anti-commutation relations (B.11) and the fact that operators $P_i^{(k)}$ for $P \in \{X,Y,Z\}$ are reflections, defined by property ${P_i^{(k)}}^2 = \mathbb{1}$ on the support of $|\psi\rangle$.

Premise $\bar{q}_1 \neq \bar{q}_2$ leads to conclusion $|\xi_{\bar{q}}\rangle = 0$. In a completely analogous way, starting from eq. (C.11) one can show that $|\xi_{\bar{q}}\rangle = 0$ if there exists l such that $\bar{q}_{2l-1} \neq \bar{q}_{2l}$. Similarly, eq. (C.12) can be used to prove that $|\xi_{\bar{q}}\rangle = 0$ if there exists l such that $\bar{q}_{2l} \neq \bar{q}_{2l+1}$. The only two states $|\bar{q}\rangle$ which satisfy $\bar{q}_{2l-1} = \bar{q}_{2l} = \bar{q}_{2l+1}$ are $|\bar{q}\rangle = |0\dots0\rangle$ and $|\bar{q}\rangle = |1\dots1\rangle$. This means that

$$|\xi\rangle = |\xi_0\rangle \otimes |0\dots0\rangle + |\xi_1\rangle \otimes |1\dots1\rangle\,, \tag{C.14}$$

which is exactly what had to be proven.

Appendix D

Entanglement certification proofs

D.1 Positivity of $\mathscr{I}$ for separable states: qubits

Our aim is to prove that under maximal violation in step (ii) of the protocol

$$\mathscr{I} = \sum_{cduw} \omega_{cd}^{zw}\, p(c,+,+,d|z,x=\star,y=\star,w) \geq 0, \tag{D.1}$$

holds for all separable ρ^{AB}. First, note that the projectors for Charlie's measurement can be compactly written

$$\Pi_{c|z}^{\mathrm{C'C''}} = U_{\mathrm{C}}^{\dagger} \sum_{j} \left(\pi_{c|z}^{\mathrm{C'}}\right)^{T^{j}} \otimes |j\rangle\langle j|^{\mathrm{C''}} U_{\mathrm{C}}, \tag{D.2}$$

where U_{C} is the local unitary from lemma 1 and $\pi_{c|z}$ are projectors onto the Pauli eigenvectors, i.e. $\pi_{c|z} = \frac{1}{2}[\mathbb{1} + c\sigma_z]$ for $\sigma_z = \sigma_{\mathrm{Z}}, \sigma_{\mathrm{X}}, \sigma_{\mathrm{Y}}$. Thus, at maximum violation, the (sub-normalized) states that Alice receives in the $\rangle_0$ spaces conditional on a certain c,z are given by

$$\tau_{c|z} = \frac{1}{2} U_{\mathrm{A}}^{\dagger} \left[\sum_{j} \rho_{\xi}^{j} \otimes (\pi_{c|z}^{\mathrm{A}_0'})^{T_j}\right] U_{\mathrm{A}}, \tag{D.3}$$

where

$$\rho_{\xi}^{j} = \mathrm{tr}_{\mathrm{C''CC'}} \left[|j\rangle\langle j|^{\mathrm{C''}}\, |\mathrm{junk}\rangle\langle\mathrm{junk}|^{\mathrm{C''CA_0''A_0}}\right]. \tag{D.4}$$

Here, we have used the property $\mathrm{tr}_{\mathrm{C}}[|\Phi^{+}\rangle\langle\Phi^{+}|C \otimes \mathbb{1}] = C^{T}$. We thus have

$$\begin{aligned} p(c,+,+,d|z,x=\star,y=\star,w) &= \mathrm{tr}\left[\mathsf{M}_{+|\star}^{\mathrm{A_0A}} \otimes \mathsf{M}_{+|\star}^{\mathrm{B_0B}}, \tau_{c|z} \otimes \rho^{\mathrm{AB}} \otimes \tau_{d|w}\right] \qquad \text{(D.5)} \\ &= \sum_{j,k} \mathrm{tr}\left[\mathrm{A} \otimes \mathrm{B}, \rho_{\mathrm{junk}}^{j} \otimes (\pi_{c|z}^{\mathrm{A}_0'})^{T_j} \otimes \rho^{\mathrm{AB}} \otimes (\pi_{d|w}^{\mathrm{B}_0'})^{T_k} \otimes \rho_{\mathrm{junk}}^{k}\right], \qquad \text{(D.6)} \end{aligned}$$

where $\mathrm{A} = \frac{1}{2}U_\mathrm{A}\mathsf{M}^{\mathrm{A}_0\mathrm{A}}_{+|\star}U_\mathrm{A}^\dagger$, $\mathrm{B} = \frac{1}{2}U_\mathrm{B}\mathsf{M}^{\mathrm{B}\mathrm{B}_0}_{+|\star}U_\mathrm{B}^\dagger$. Now, assume that ρ^{AB} is product so that $\rho^{\mathrm{AB}} = \sigma^\mathrm{A} \otimes \sigma^\mathrm{B}$ (mixtures of such states will be considered later). Then the above takes the form

$$\sum_{j,k} \mathrm{tr}\left[\pi^{T_j}_{c|z} \otimes \pi^{T_k}_{d|w} \mathrm{A}_j \otimes \mathrm{B}_k\right] \tag{D.7}$$

where

$$\mathrm{A}_j = \mathrm{tr}_{\mathrm{AA}_0\mathrm{A}_0''}\left[\mathrm{A}\,\rho^j_{\mathrm{junk}} \otimes \mathbb{1}_{\mathrm{A}_0'} \otimes \sigma^\mathrm{A}\right]; \quad \mathrm{B}_k = \mathrm{tr}_{\mathrm{BB}_0\mathrm{B}_0''}\left[\mathrm{B}\,\sigma^\mathrm{B} \otimes \mathbb{1}_{\mathrm{B}_0'} \otimes \rho^k_{\mathrm{junk}}\right]. \tag{D.8}$$

Note that A_j and B_k are positive operators since A_j can be seen as a positive map applied to $\sigma^\rangle$. Using this we may now write $\mathscr{I}$ as

$$\begin{aligned}
\mathscr{I} &= \sum_{jk}\sum_{cdzw} \omega^{zw}_{cd}\,\mathrm{tr}\left[\pi^{T_j}_{c|z} \otimes \pi^{T_k}_{d|w} \mathrm{A}_j \otimes \mathrm{B}_k\right] && \text{(D.9)}\\
&= \sum_{jk}\sum_{cdzw} \omega^{zw}_{cd}\,\mathrm{tr}\left[\pi_{c|z} \otimes \pi_{d|w} \mathrm{A}_j^{T_j} \otimes \mathrm{B}_k^{T_k}\right] && \text{(D.10)}\\
&= \sum_{jk} \mathrm{tr}\left[\mathscr{W}\,\mathrm{A}_j^{T_j} \otimes \mathrm{B}_k^{T_k}\right] \geq 0, && \text{(D.11)}
\end{aligned}$$

where the second equality follows from $\mathrm{tr}[X] = \mathrm{tr}[X^T]$, and the final inequality follows from the fact that $\mathrm{A}_j^{T_j}$ and $\mathrm{B}_k^{T_k}$ are positive operators and thus $\mathrm{A}_j^{T_j} \otimes \mathrm{B}_k^{T_k}$ is a unnormalized product state. Since $\mathscr{I}$ is linear in $\rho^{\rangle\mathrm{B}}$ one also has $\mathscr{I} \geq 0$ for mixtures of product states and thus all separable states.

D.2 Positivity of $\mathscr{I}$ for separable states: arbitrary dimension

The proof follows the same structure as for the qubit case. As a consequence of Lemma 9.7, we have that Alice receives the subnormalized steered states conditioned on **z**, **c**:

$$\tau_{\mathbf{c},\mathbf{z}} = \frac{1}{d} U_\mathrm{A}^\dagger \left[\sum_{j=0}^{1} \rho^j_\xi \otimes \left(\pi^{\mathrm{A}_0'}_{\mathbf{c}|\mathbf{z}}\right)^{T^j}\right] U_\mathrm{A}, \tag{D.12}$$

where we define

$$\pi^{\mathrm{A}_0'}_{\mathbf{c}|\mathbf{z}} = \otimes_i \pi^{\mathrm{A}_{0i}'}_{c_i|z_i} \qquad \text{and} \qquad \rho^j_\xi = \mathrm{tr}_{\mathrm{C}''\mathrm{CC}'}\left[(\otimes_i |j\rangle\langle j|^{\mathrm{C}_i''})\,|\xi\rangle\langle\xi|^{\mathrm{C}''\mathrm{CA}_0''\mathrm{A}_0}\right]. \tag{D.13}$$

and Bob has analogous states conditioned on Daisy's input and output. Now, the probabilities are given by

$$p(\mathbf{c},+,+,\mathbf{d}|\mathbf{z},x=\star,y=\star,\mathbf{w}) = \mathrm{tr}\left[\mathsf{M}^{\mathrm{A_0A}}_{+|\star}\otimes\mathsf{M}^{\mathrm{B_0B}}_{+|\star}\,\tau_{\mathbf{c}|\mathbf{z}}\otimes\rho^{\mathrm{AB}}\otimes\tau_{\mathbf{d}|\mathbf{w}}\right] \tag{D.14}$$

$$= \sum_{j,k}\mathrm{tr}\left[\mathrm{A}\otimes\mathrm{B}\,\rho^{j}_{\xi}\otimes(\pi^{\mathrm{A}_0'}_{\mathbf{c}|\mathbf{z}})^{T_j}\otimes\rho^{\mathrm{AB}}\otimes(\pi^{\mathrm{B}_0'}_{\mathbf{d}|\mathbf{w}})^{T_k}\otimes\rho^{k}_{\xi}\right], \tag{D.15}$$

and $A = \frac{1}{d}U_{\mathrm{A}}\mathsf{M}^{\mathrm{A_0A}}_{+|\star}U^{\dagger}_{\mathrm{A}}$, $\mathrm{B} = \frac{1}{d}U_{\mathrm{B}}\mathsf{M}^{\mathrm{BB_0}}_{+|\star}U^{\dagger}_{\mathrm{B}}$. For separable $\rho^{\rangle\mathrm{B}} = \sigma^{\rangle}\otimes\sigma^{\mathrm{B}}$ this takes the form

$$p(\mathbf{c},+,+,\mathbf{d}|\mathbf{z},x=\star,y=\star,\mathbf{w}) = \sum_{j,k}\mathrm{tr}\left[\pi^{T_j}_{\mathbf{c}|\mathbf{z}}\otimes\pi^{T_k}_{\mathbf{d}|\mathbf{w}}\,\mathrm{A}_j\otimes\mathrm{B}_k\right] \tag{D.16}$$

where again we have the positive operators

$$\mathrm{A}_j = \mathrm{tr}_{\mathrm{AA_0A_0''}}\left[\mathrm{A}\,\rho^{j}_{\xi}\otimes\mathbb{1}_{\mathrm{A}_0'}\otimes\sigma^{\mathrm{A}}\right]; \quad \mathrm{B}_k = \mathrm{tr}_{\mathrm{BB_0B_0''}}\left[\mathrm{B}\,\sigma^{\mathrm{B}}\otimes\mathbb{1}_{\mathrm{B}_0'}\otimes\rho^{k}_{\xi}\right]. \tag{D.17}$$

Hence we find

$$\mathscr{I} = \sum_{jk}\sum_{\mathbf{cdzw}}\omega^{\mathbf{zw}}_{\mathbf{cd}}\,\mathrm{tr}\left[\pi^{T_j}_{\mathbf{c}|\mathbf{z}}\otimes\pi^{T_k}_{\mathbf{d}|\mathbf{w}}\,\mathrm{A}_j\otimes\mathrm{B}_k\right] \tag{D.18}$$

$$= \sum_{jk}\sum_{\mathbf{cdzw}}\omega^{\mathbf{zw}}_{\mathbf{cd}}\,\mathrm{tr}\left[\pi_{\mathbf{c}|\mathbf{z}}\otimes\pi_{\mathbf{d}|\mathbf{w}}\,\mathrm{A}^{T_j}_j\otimes\mathrm{B}^{T_k}_k\right] \tag{D.19}$$

$$= \sum_{jk}\mathrm{tr}\left[\mathscr{W}\,\mathrm{A}^{T_j}_j\otimes\mathrm{B}^{T_k}_k\right] \geq 0. \tag{D.20}$$

Again, due to the linearity of $\mathscr{I}$ in ρ^{AB}, one has $\mathscr{I} \geq 0$ for all separable states, completing the proof.

Bibliography

[Aci+07] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani,*Device-independent security of quantum cryptography against collective attacks* Phys. Rev. Lett. **98**:230501 (2007).

[AGT06] A. Acín, N. Gisin, and B. Toner, *Grothendieck's constant and local models for noisy entangled quantum states*, Phys. Rev. A **73** (2006).

[AM16] A. Acín, L. Masanes, *Certified randomness in quantum physics* Nature **540**, 213–219, (2016).

[AMP12] A. Acín, S. Massar, S. Pironio, *Randomness versus Nonlocality and Entanglement*, Phys. Rev. Lett. **108**, 100402 (2012).

[APVW16] A. Acín, S. Pironio, T. Vértesi, P. Wittek, *Optimal randomness certification from one entangled bit*, Phys. Rev. A, **93**, 040102 (2016)

[And+17] O. Andersson, P. Badziag, I. Bengtsson, I. Dumitru, A. Cabello, *Self-testing properties of Gisin's elegant Bell inequality*, Phys. Rev. A **96**, 032119 (2017)

[Ard92] M. Ardehali, *Bell inequalities with a magnitude of violation that grows exponentially with the number of particles* Phys. Rev. A **46**, 5375 (1992).

[AFR16] R Arnon-Friedman, R Renner, T Vidick, *Simple and tight device-independent security proofs*, Preprint at arXiv:1607.01797 [quant-ph] (2016)

[ADR81] A. Aspect, J. Dalibard, and G. Roger,*Experimental Test of Bell's Inequalities Using Time-Varying Analyzers* Phys. Rev. Lett. **49**, 1804, (1982).

[ADTA15] R. Augusiak, M. Demianowicz, J. Tura, A. Acín, *Entanglement and Nonlocality are Inequivalent for Any Number of Parties*, Phys. Rev. Lett. **115** (3), 030404, (2015).

[BP15] 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 **91** 052111, (2015).

[BNSTY15] J. D. Bancal, M. Navascués, V. Scarani, T Vértesi, T. H. Yang. *Physical characterization of quantum devices from nonlocal correlations*, Phys. Rev. A **91** (2), 022115, (2015)

[BSS14] J. D. Bancal, L. Sheridan, V. Scarani, *More randomness from the same date*, New J. Phys. **16** 033011 (2014).

[Bar02] J. Barrett, *Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality*, Phys. Rev. A **65** 042302 (2002).

[BHK05] J. Barrett, L. Hardy, A. Kent, *No singalling and quantum key distribution*, Phys. Rev. Lett. **95**, 010503 (2005)

[BKP06] J. Barrett, A. Kent, S. Pironio, *Maximally Nonlocal and Monogamous Quantum Correlations*, Phys. Rev. Lett. **97**, 170409 (2006)

[BSP14] T. Baumgratz, M. Cramer, M. B. Plenio, *Quantifying coherence*, Phys. Rev. Lett. **113**, 140401 (2014)

[BK93] A. V. Belinsky and D. N. Klyshko, *Interference of light and Bell's theorem* Sov. Phys. Usp. **36**, 653 (1993).

[Bell64] J. S. Bell, *On the Einstein-Podolsky-Rosen paradox*, Physics **1**, (1964).

[BV17] E. Bene, T. Vertesy, *Measurement incompatibility does not give rise to Bell violation in general*, arXiv:1705.10069 [quant-ph] (2017)

[BBPS96] C. H. Bennett, H. J. Bernstein, S. Popescu, B. Schumacher, *Concentrating Partial Entanglement by Local Operations*, Phys. Rev. A. 53: 2046–2052 (1996).

[Ben+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895 (1993).

[Ben+96] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, W. Wootters, *Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*, Phys. Rev. Lett. 76: 722–725, (1996).

[BDSW96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-state entanglement and quantum error correction*, Phys. Rev. A 54, 3824 (1996).

[Ben+01] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, *Remote state preparation*, Phys. Rev. Lett. **87**, 077902 (2001)

[Ben+99] C. H. Bennet, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A Smolin, B. Terhal, *Unextendible product bases and bound entanglement*, Phys. Rev. Lett. **82**, 5385 (1999)

[BW92] C. H. Bennett, S. Wiesner, *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Phys. Rev. Lett. **69** (20): 2881, (1992)

[Bia+17] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, S. Lloyd, *Quantum machine learning*, Nature **549**, 195–202, (2017)

[Bos+98] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, *Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels* Phys. Rev. Lett. **80**, 1121 (1998).

[Bow+97] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Experimental quantum teleportation*, Nature **390**, 575-579 (1997)

[BŠCA18] J. Bowles, I. Šupić, D. Cavalcanti, A. Acín,*Device-independent entanglement certification of all entangled states*, arXiv:1801.10444, (2018)

[BŠCA18a] J. Bowles, I. Šupić, D. Cavalcanti, A. Acín,*Self-testing of Pauli observables for device-independent entanglement certification* arXiv:1801.10446, (2018)

[BVQB14] J. Bowles, T. Vértesi, M. T. Quintino, N. Brunner, *One-way einstein-podolsky-rosen steering* Phys. Rev. Lett. **112** (20), 200402, (2014)

[BV04] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge University Press (2004)

[BRLG13] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, *Measurement-device-independent entanglement witnesses for all entangled quantum states*, Phys. Rev. Lett. **110**, 060405 (2013)

[Bra+12] 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 **85**, 010301 (2012).

[BLMS00] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Limitations on practical quantum cryptography*, Phys. Rev. Lett. **85**, 1330, (2000).

[BC90] S. L. Braunstein and C. Caves, *Wringing out better Bell inequalities* Ann. Phys. (NY) **202** 22 (1990).

[BP12] S. L. Braunstein, S. Pirandola, *Side-Channel-Free Quantum Key Distribution*, Phys. Rev. Lett. **108**, 130502 (2012).

[BDCZ98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum repeaters: the role of imperfect local operations in quantum communication*, Phys. Rev. Lett. **81**, 5932 (1998)

[BFK09] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Universal blind quantum computation*, Proc. of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), 517-526 (2009).

[BCPSW14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Whener, *Bell nonlocality*, Rev. Mod. Phys. **86**, 419 (2014)

[Bru+08] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, V. Scarani, *Testing the dimension of Hilbert spaces*, Phys. Rev. Lett. **100** (21), 210503, (2008)

[BNS17] K. Bu, N. Anand, and U. Singh, *Asymmetry and coherence weight of quantum states*, arXiv preprint 1703.01266 [quant-ph] (2017)

[Bus12] F. Buscemi, *All entangled quantum states are nonlocal*, Phys. Rev. Lett. **108**, 200401 (2012)

[CABV13] D. Cavalcanti, A. Acín, N. Brunner, T. Vértesi, *All quantum states useful for teleportation are nonlocal resources*, Phys. Rev. A **8**7, 042104 (2013)

[Cav+15] D. Cavalcanti, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. Souto Ribeiro, and S. P. Walborn, *Detection of entanglement in asymmetric quantum networks and multipartite quantum steering*, Nat. Commun. **6**, 7941 (2015)

[CB15] A. Chaturvedi and M. Banik, *Measurement-device-independent randomness from local entangled states*, Europhysics Letters **112**(3), 30003 (2015)

[CSŠ17] D. Cavalcanti, P. Skrzypczyk,I. Šupić, *All Entangled States can Demonstrate Nonclassical Teleportation*, Phys. Rev. Lett. **119** (11), 110501, (2017).

[CS17] D. Cavalcanti and P. Skrzypczyk, *Quantum steering: a short review with focus on semidefinite programming*, Rep. Prog. Phys. **80** 024001 (2017).

[CHW13] E. G. Cavalcanti, M. J. W. Hall, H. M. Wiseman, *Entanglement verification and steering when Alice and Bob cannot be trusted* Phys. Rev. A **87**, 032306 (2013)

[CJWR09] 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 **80**, 032112, (2009).

[Chi+12] A. Chiuri, C. Greganti, M. Paternostro, G. Vallone, and P. Mataloni, *Experimental quantum networking protocols via four-qubit hyperentangled Dicke states* Phys. Rev. Lett. **109**, 173604 (2012).

[CW03] M. Christandl, A. Winter, *"Squashed Entanglement" - an Additive Entanglement Measure*, J. Math. Phys. **45** (3):829, (2003) [CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**:880, (1969).

[CGL99] R. Cleve,D. Gottesman, and H.-K. Lo, *How to share a quantum secret*, Phys. Rev. Lett. **83**, 648 (1999)

[CHTW04] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, *Consequences and Limits of Nonlocal Strategies*, Proc. of the 19th Annual IEEE Conf. on Computational Complexity, p 236-249, (2004)

[Col17] A. Coladangelo, *Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH*, Quan. Inf. Comp. **17** (9,10)7(2017).

[CGS17] A. Coladangelo, K. T. Goh, V. Scarani, *All pure bipartite entangled states can be self-tested*, Nature Communications 8, 15485 (2017).

[CGJV17] A. Coladangelo, A. Grilo, S. Jeffery, T. Vidick, *Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources*, arXiv:1708.07359 (2017)

[CK11] R. Colbeck,*PhD Thesis, under the supervision of A. Kent, University of Cambridge* (2006); R. Colbeck and A. Kent, *J. Phys. A Math. Gen.*, **44**(9):095305 (2011).

[CN16] M. Coudron, A. Natarajan, *The Parallel-Repeated Magic Square Game is Rigid*, arXiv:1609.06306 (2016).

[CZM15] Z. Cao, H. Zhou and X. Ma, *Loss-tolerant measurement-device-independent quantum random number generation*, New J. Phys. **17**, 125011 (2015);

[DFR16] F. Dupuis, O. Fawzi, R. Renner, *Entropy accumulation*, arXiv:1607.01796 (2016)

[DGS77] P. Delsarte, J. M. Goethals, and J. J. Seidel, *Spherical codes and designs*, Geom. Dedicata **6** , 363-388 (1977)

[DPA13] C. Dhara, G. Prettico, and Antonio Acín, *Maximal quantum randomness in Bell tests*, Phys. Rev. A **88**, 052116, (2013).

[DPP05] G.M. D'Ariano, P. Lo Presti, and P. Perinotti, *Classical randomness in quantum measurements*, J. Phys. A, **38**:5979–5991 (2005)

[DŠHA18] L. Domingo Colomer, I. Šupić, M. Hoban, A. Acín, *Measurement-device-independent quantum state certification*, *in preparation* (2008)

[Doh14] A. C. Doherty, *Entanglement and shareability of quantum states*, J. Phys. A: Math. Theor. **47**, 424004 (2014)

[DPS02] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, *Distinguishing separable and entangled states*, Phys. Rev. Lett. **88**(18), 187904 (2002)

[DPS04] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, *Complete family of separability criteria*, Phys. Rev. A **69**(2), 022308 (2004)

[EPR35] A. Einstein, B. Podolsky, N. Rosen, *Can Quantum-Mechanical Description of Physical Reality be Considered Complete?*, Phys. Rev. **47** (10): 777–780, (1935).

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

[Fine82] A. Fine, *Hidden Variables, Joint Probability, and the Bell Inequalities*, Phys. Rev. Lett. **48**, 291, (1982)

[FFW11] T. Franz, F. Furrer and R.F. Werner, *Extremal quantum correlations and cryptographic security*, Phys. Rev. Lett. **106**:250502

[FC72] S. Freedman, and J. Clauser, *Experimental Test of Local Hidden-Variable Theories* Phys. Rev. Lett. **28**, 938, (1972)

[Fur+98] A. Furusawa, et al. *Unconditional quantum teleportation*, Science **282**, 706–709 (1998).

[GWK17] A. Gheorghiu, P. Wallden, and E. Kashefi, *Rigidity of quantum steering and one-sided device-independent verifiable quantum computation*, New J, Phys. **19** (2), (2017)

[GBHA10] R. Gallego, N. Brunner, C. Hadley, and A. Acin, *Device-independent tests of classical and quantum dimensions* Phys. Rev. Lett. **105**, 230501 (2010)

[Gis91] N. Gisin, *Bell's inequality holds for all non-product states*, Phys. Lett. A **154**, 201, (1991).

[GRTZ02] N. Gisin, G. Ribordy, W. Titel, and H. Zbinden, *Quantum cryptography*, Rev. Mod. Phys. **74**, 145 (2002)

[Giu+15] M. Giustina, et al. , *Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons*, Phys. Rev. Lett. **115**, 250401, (2015).

[GC99] D. Gottesman and I. L. Chuang, *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations*, Nature **402**, 390 (1999)

[GHZ89] D. M. Greenberger, M. A. Horne, A. Zeilinger, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by Kafatos M. (Kluwer, Dordrecht), p. 69, (1989).

[GHSZ90] D. M. Greenberger, M. A. Horne, A. Shimony and A. Zeilinger, *Bell's theorem without inequalities*, Am. J. Phys. **58**, 1131 (1990).

[Güh+02] O. Gühne , P. Hyllus , D. Bruss , A. Ekert , M. Lewenstein , C. Macchiavello , A. Sanpera, *Detection of entanglement with few local measurements*, Phys. Rev. A **66**, 062305 (2002).

[GT09] O. Gühne, G. Toth, *Entanglement detection*, Phys. Rep. **474** (1), 1-75, (2009)

[Gur04] L. Gurvits, *Classical complexity and quantum entanglement*, J. Comp. Sys. Sci., **69**:448, (2004);

[Hal16] M. J. W. Hall, *Trust-free verification of steering: why you can't cheat a quantum referee*, arXiv:1606.00196 [quant-ph] (2016)

[HN03] A. W. Harrow and M. A. Nielsen, *How robust is a quantum gate in the presence of noise?* Phys. Rev. A **68**, 012308 (2003)

[HHT01] P. M. Hayden, M. Horodecki, B. M. Terhal, *The asymptotic entanglement cost of preparing a quantum state*, J. Phys. A: Mathematical and General **34**, 6891, (2001).

[Hei+06] M. Hein, W. Dür, J. Eisert, R. Raussendor, M. van den Nest and H.-J. Briegel, *Entanglement in graph states and its applications*, Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos (2006).

[HEB04] M. Hein, J. Eisert, H. J. Briegel,*Multiparty entanglement in graph states* Phys. Rev. A **69**, 062311 (2004).

[Hen+15] B. Hensen, et al. , *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres* Nature **526**, 682 (2015).

[HBB99] M. Hillery,V. Buzek, and A. Berthiaume, *Quantum secret sharing*, Phys. Rev. A **59**, 1829 (1999)

[HW97] S. Hill and W. K. Wooters, *Entanglement of a Pair of Quantum Bits*, Phys. Rev. Lett. **78**, 5022 (1997).

[Hir+16] F. Hirsch, M. T. Quintino, J. Bowles, T. Vértesi, and N. Brunner, *Entanglement without hidden nonlocality* New J. Phys. **18** 113019 (2016)

[HQB17] F. Hirsch, M. T. Quintino, N. Brunner, *Quantum measurement incompatibility does not imply Bell nonlocality*, arXiv:1707.06960 [quant-ph] (2017)

[HCLB11] M. J. Hoban, E. T. Campbell, K. Loukopoulos, and D. E. Browne, *Non-adaptive measurement-based quantum computation and multi-party Bell inequalities*, New J. Phys. **13** 023014 (2011).

[HS17] M. J. Hoban and A. B. Sainz, *A channel-based framework for steering, non-locality and beyond*, arXiv preprint 1708.00750 [quant-ph]

[Hor97] P. Horodecki *Separability criterion and inseparable mixed states with positive partial transposition* Phys. Lett. A, **232**:333, (1997)

[HHH96] M. Horodecki, P. Horodecki, R. Horodecki, *Separability of mixed states: necessary and sufficient conditions*, Phys. Lett. A. **223** (1-2): 1–8, (1996).

[HHH99] M. Horodecki, P. Horodecki, and R. Horodecki, *General teleportation channel, singlet fraction, and quasidistillation*, Phys. Rev. A **60**, 1888 (1999)

[HHHH09] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum entanglement*, Rev. Mod. Phys. **81**, 865, (2009).

[HJW93] L. P. Hughston, R. Jozsa, and W. K. Wootters, *A complete classification of quantum ensembles having a given density matrix*, Phys. Lett. A **183**, 14–18, (1993).

[JPOK03] J. Joo, Y.-J. Park, S. Oh, and J. Kim, *Quantum teleportation via a W state*, New Journal of Physics **5**, 136, (2003)

[Kan16] J. Kaniewski, *Analytic and (nearly) optimal self-testing bounds for the Clauser-Holt-Shimony-Horne and Mermin inequalities*, Phys. Rev. Lett. **117**, 070402 (2016).

[Kan17] J. Kaniewski, *Self-testing of binary observables based on commutation*, Phys. Rev. A, **95**, 062323 (2017).

[KB98] A. Karlsson, M. Bourennane, *Quantum teleportation using three-particle entanglement*,Phys. Rev. A **58** (6), 4394 (1998)

[KSCAA15] 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. **115** 210401 (2015).

[Kre89] E. Kreyszig, *Introductory Functional Analysis with Applications*, Vol. 17 of Wiley Classics Library, Wiley (1989)

[Kri+11] R. Krischek, C. Schwemmer, W. Wieczorek, H. Weinfurter, P. Hyllus, L. Pezze, and A. Smerzi, *Useful multiparticle entanglement and sub-shot-noise sensitivity in experimental phase estimation*, Phys. Rev. Lett. **107**, 080504 (2011).

[LTBS14] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, *Quantum randomness extraction for various levels of characterization of the devices* J. Phys. A: Math. Theor. **47**, 424028 (2014)

[LS98] M. Lewenstein and A. Sanpera, *Separability and Entanglement of Composite Quantum Systems,* Phys. Rev. Lett. 80, 2261 (1998).

[LPTRG13] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, N. Gisin, *Device-Independent Quantum Key Distribution with Local Bell Test*, Phys. Rev. X **3**, 031006 (2013)

[LCQ12] H.-K. Lo, M. Curty, B. Qi, *Measurement-device-independent quantum key distribution*, Phys. Rev. Lett. **108**, 130503 (2012).

[MMMO06] F. Magniez, D. Mayers, M. Mosca and H Ollivier, *Self-testing of quantum circuits* Automata, Languages and Programming, (Springer Berlin Heidelberg) p 72-83, (2006)

[MS16] I. Marvian and R. Spekkens, *How to quantify coherence: Distinguishing speakable and unspeakable notions*, Phys. Rev. A **94** 052324 (2016)

[Mat+17] A. Mattar *et al*, *Experimental multipartite entanglement and randomness certification of the W state in the quantum steering scenario*, Quantum Sci. Technol. **2** 015011, (2017)

[MY04] D. Mayers and A. Yao, *Self-testing quantum apparatus*, Quant. Inf. Comput. **4**, 273 (2004).

[McK14] M. McKague, *Self-Testing Graph States* Theory of Quantum Computation, Communication, and Cryptography: 6th Conference, TQC 2011, Madrid, Spain, May 24-26, 2011, Revised Selected Papers, pages 104-120. Springer Berlin Heidelberg, Berlin, Heidelberg (2014).

[McK17] M. McKague, *Self-testing in parallel with CHSH*, Quantum **1**, 1, (2017).

[McKM11] M. McKague and M. Mosca, *Generalized self-testing and the security of the 6-state protocol*, Theory of Quantum Computation, Communication, and Cryptography: 5th Conference, TQC 2010, p 113-130, (2011)

[MYS14] M. McKague, T. H. Yang, V. Scarani, *Robust self-testing of the singlet* J. Phys. A: Math. Theor. **45**, 455304 (2014).

[Mer90] N.D.Mermin, *Extreme quantum entanglement in a superposition of macroscopically distinct states* Phys.Rev.Lett., **65**, 1838 (1990).

[MS12] C. Miler, Y. Shi, *Optimal robust quantum self-testing by binary nonlocal XOR games*, arxiv:1207.1819 [quant-ph], (2012)

[Mor+13] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, *Device-Independent Entanglement Quantification and Related Applications*, Phys. Rev. Lett. **111**, 030501 (2013);

[Nap+16] C. Napoli, T. R. Bromley, M. Cianciaruso, M. Piani, N. Johnston, and G. Adesso, *Robustness of Coherence: An Operational and Observable Measure of Quantum Coherence*, Phys. Rev. Lett. **116** 150502 (2016)

[NDV14] M. Navascués, G. de la Torre, and T. Vértesi, *Characterization of quantum correlations with local dimension constraints and its device-independent applications* Phys. Rev. X **4**, 011011 (2014)

[Nie+16] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, *Experimental measurement-device-independent quantum random-number generation*, Phys. Rev. A **94**, 060301 (2016)

[NPA07] M. Navascués, S. Pironio, and A. Acín, *Bounding the set of quantum correlations*, Phys. Rev. Lett. **98**, 010401 (2007); M. Navascués, S. Pironio, and A. Acín, *A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations* New J. Phys. **10** (7), 073013 (2008)

[NMAB15] M. Nawareg, S. Muhammad, E. Amselem, and M. Bourennane, *Experimental Measurement-Device-Independent Entanglement Detection*, Scientific Reports **5**, 8048 (2015)

[NC00] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[NSPS13] O. Nieto Silleras, S. Pironio and J. Silman, *Using complete measurement statistics for optimal device-independent randomness evaluation*, New. J. Phys. **16** 013035 (2013).

[PVN14] K. F. Pál, T. Vértesi, M. Navascués, *Device-independent tomography of multipartite quantum states*, Phys. Rev. A **90**, 042340 (2014).

[Pal12] C. Palazuelos, *Superactivation of quantum nonlocality*, Phys. Rev. Lett. **109**, 190401 (2012).

[PCWDK12] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, *Multipartite entanglement verification resistant against dishonest parties* Phys. Rev. Lett. **108**, 260502 (2012).

[PCPA15] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, *Optimal randomness certification in the quantum steering and prepare-and-measure scenarios* New J. Phys. **17**, 113010 (2015)

[Pat00] A. K. Pati, *Minimum classical bit for remote preparation and measurement of a qubit*, Phys. Rev. A **63**,014302 (2000).

[PB11] M. Pawlowski, and N. Brunner, *Semi-device-independent security of one-way quantum key distribution* Phys. Rev. A **84**, 010302(R) (2011)

[Pea70] P. A. Pearle, *Phys. Rev. D* **2**, 1418, (1970); S. L. Braunstein and C. Caves, *Ann. Phys. (NY)* **202** 22, (1990).

[Per96] A. Peres, *Separability Criterion for Density Matrices*, Phys. Rev. Lett. 77, 1413–1415 (1996)

[Pir+10] S. Pironio et al., *Random numbers certified by Bell's theorem*, Nature **464** (7291), 1021-1024, (2010)

[Ple05] M. B. Plenio, *Logarithmic Negativity: A Full Entanglement Monotone That is not Convex* Phys. Rev. Lett. **95**, 090503 (2005).

[PV07] M. B. Plenio and S. Virmani, *An introduction to entanglement measures* Quant. Info. Comp. **7**:1-51 (2007)

[PM95] S. Popescu, and S. Massar, *Optimal extraction of information from finite quantum ensembles*, Phys. Rev. Lett. **74**, 1259–1263 (1995)

[Pop94] S. Popescu, *Bell's inequalities versus teleportation: What is nonlocality?*, Phys. Rev. Lett. **72**, 797 (1994)

[Pop95] S. Popescu, *Bell's inequalities and density matrices: revealing hidden nonlocality*, Phys. Rev. Lett. **74**, 2619 (1995)

[Pre18] J. Preskill, *Quantum Computing in the NISQ era and beyond*, arXiv:1801.00862 (2018).

[Pre+09] R. Prevedel, G. Cronenberg, M. S. Tame, M. Paternostro, P. Walther, M. S. Kim, and A. Zeilinger, *Experimental realization of Dicke states of up to six qubits for multiparty quantum networking*, Phys. Rev. Lett. **103**, 020503 (2009).

[Pus15] M. F. Pusey, *Verifying the quantumness of a channel with an untrusted device*, J. Opt. Soc. Am. B **32** A56 (2015)

[Qui+15] M. T. Quintino, T. Vértesi, D. Cavalcanti, R. Augusiak, M. Demianowicz, A. Acín, and N. Brunner, *Inequivalence of entanglement, steering, and Bell nonlocality for general measurements*, Phys. Rev. A **92**, 032107, (2015) [Rab+11] R. Rabelo, M. Ho, D. Cavalcanti, N. Brunner, V. Scarani, *Device-independent certification of entangled measurements*, Phys. Rev. Lett. **107** (5), 050502, (2011)

[RB01] R. Raussendorf and H.-J. Briegel, *A one-way quantum computer*, Phys. Rev. Lett. **86**, 5188 (2001)

[RUV13] B. Reichardt, F. Unger and U. Vazirani, *Classical command of quantum systems*, Nature, **496**:456-460 (2013).

[RBGL13] D. Rosset, C. Branciard, N. Gisin, Y.-C. Liang, *Correlations of entangled quantum states cannot be classically simulated*, New J. Phys. **15**, 053025 (2013)

[Ros+12] D. Rosset, R.l Ferretti-Schöbitz, J.-D, Bancal, N. Gisin, Y.-C. Liang, *Imperfect measurements settings: implications on quantum state tomography and entanglement witnesses*, Phys. Rev. A **86**, 062325 (2012)

[Ruk+10] Rukhin, A. et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Special Publication 800-22 rev1a, National Institute of Standards and Technology (2010).

[Sal+17] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A Acín, S. Pironio, *Bell inequalities tailored to maximally entangled states*, Phys. Rev. Lett. **119**, 040402 (2017)

[Sch35] E. Schrödinger, *Discussion of probability relations between separated systems*, Math. Proc. Camb. Phil. Soc. **31** (4): 555–563, (1935)

[Sch36] E. Schrödinger, *Probability relations between separated systems*, Math. Proc. Camb. Phil. Soc. **32**, 446–452, (1936).

[SBBZ05] A. Sen De, U. Sen, C. Brukner, V. Buzek, and M. Zukowski, *Entanglement swapping of noisy states: A kind of superadditivity in nonclassicality*, Phys. Rev. A **72**, 042310 (2005).

[SHR17] F. Shahandeh, M. J. W. Hall, and T. C. Ralph, *Measurement-Device-Independent Approach to Entanglement Measures*, Phys. Rev. Lett. **118**, 150505 (2017)

[Sha+15] L. K. Shalm et al. , *Strong Loophole-Free Test of Local Realism*, Phys. Rev. Lett. **115**, 250402 (2015).

[Sha48] Shanon C. E. *A Mathematical Theory of Communication*, Bell System Technical Journal. **27** (3): 379–423, (1948).

[SNC14] P. Skrzypczyk, M. Navascués, D. Cavalcanti, *Quantifying Einstein-Podolsky-Rosen steering*, Phys. Rev. Lett. **12**, 180404 (2014)

[Ste03] M. Steiner, *Generalized robustness of entanglement*, Phys. Rev. A **67** 054305 (2003)

[ŠASA16] I Šupić, R. Augusiak, A. Salavrakos, A. Acín, *Self-testing protocols based on the chained Bell inequalities* New J. Phys., **18**, 035013, (2016).

[ŠCAA17] I. Šupić, A. Coladangelo, R. Augusiak, A. Acín, *A simple approach to self-testing multipartite states*, arXiv: 1707.06534, (2017).

[ŠH16] I Šupić, M. J. Hoban, *Self-testing through EPR-steering*, New J. Phys. **18**, 075006, (2016).

[ŠSC17] I. Šupić, P. Skrzypczyk, D. Cavalcanti, *Measurement-device-independent entanglement and randomness estimation in quantum networks*, Phys. Rev. A **95** (4), 042340, (2017).

[Ter00] B. M. Terhal, *Bell inequalities and the separability criterion*, Phys. Lett. A. **271** (5-6): 319–326, (2000).

[TBZG98] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Violation of Bell Inequalities by Photons More Than 10 km Apart* Phys. Rev. Lett. **81**, 3563, (1998).

[Tsi80] B. Tsirelson, *Quantum generalizations of Bell's inequality* Lett. Math. Phys **4**, 93 (1980).

[Tsi93] B. Tsirelson, *Some results and problems on quantum Bell-type inequalities* Hadronic Journal Supplement **8**,329-345, (1993).

[Tur37] Turing A. *On Computable Numbers, with an Application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society, **42** (1), pp. 230–65, (1937).

[Ver+16] E. Verbanis, A. Martin, D. Rosset, C. C. W. Lim, R. T. Thew, and H. Zbinden, *Resource-efficient measurement device independent entanglement witness*, Phys. Rev. Lett. **116**(19), 190501 (2016)

[Vic14] J. I. de Vicente, *On nonlocality as a resource theory and nonlocality measures*, J. Phys. A: Math. Gen. **47** , 424017 (2014)

[VT99] G. Vidal and R. Tarrach, *Robustness of entanglement*, Phys. Rev. A **59**, 141 (1999)

[VW02] G. Vidal and R. F. Werner, *A computable measure of entanglement*, Phys. Rev. A **65**, 032314 (2002)

[VV14] T. Vidick and U. Vazirani, *Fully device-independent quantum key distribution*, Phys. Rev. Lett. **113** (14), 14050, (2014) [Wal+16] N. Walk *et al*, *Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution* Optica **3** (6), 634-642, (2016).

[WWS16] Y. Wang, X. Wu and V. Scarani, *All the self-testing of singlet with two binary measurements*, New J. Phys. **18**, 025021, (2016)

[Weh06] S. Wehner, *Tsirelson bounds for generalized Clauser-Horne-Hold inequalities* Phys. Rev. A, **73**, 022110, (2006).

[Wer89] R. F. Werner, *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys. Rev. A **40**, 4277 (1989)

[WJD07] H. M. Wiseman, S. J. Jones, and A. C. Doherty, *Steering Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox*, Phys. Rev. Lett. **98** 140402 (2007).

[Wit15] P. Wittek, *Algorithm 950: Ncpol2sdpa—sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables*, ACM Transactions on Mathematical Software, **41**(3), 21, (2015).

[WBMS16] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, *Device-independent parallel self-testing of two singlets* , Phys. Rev. A **93** 062121 (2016)

[Wu+14] 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 **90**, 042339 (2014).

[Xu+14] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, *Implementation of a Measurement-Device-Independent Entanglement Witness*, Phys. Rev. Lett. **112**, 140506 (2014)

[YN13] T. H. Yang and M. Navascués, *Robust self testing of unknown quantum systems into any entangled two-qubit states*, Phys. Rev. A **87**, 050102(R) (2013).

[YVBSN14] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, M. Navascués, *Robust and versatile black-box certification of quantum devices*, Phys. Rev. Lett. **113**, 040401 (2014)

[Yan+16] X. Yang, K. Wei, H. Ma, S. Sun, H. Liu, Z. Li, Z. Yin, Y. Du, and L. Wu *Measurement-device-independent quantum secret sharing*, arxiv:1608.00114 (2016)