PhD thesis

Bell inequalities for device-independent protocols

Alexia Salavrakos

11 February 2019

Thesis supervisor: Prof. Dr. Antonio Acín

Acknowledgements

First and foremost, I would like to thank my supervisor, Antonio Acín, for giving me the great opportunity to do my PhD studies in his group. Toni created a lovely atmosphere in the QIT group and encouraged me to attend many conferences and workshops. He has been very supportive of me, and gave me a lot of freedom to perform my research as I liked.

I would also like to thank Stefano Pironio, who was my supervisor during my master's thesis, for welcoming me into the field. I am grateful for his mentoring and for being an inspiration to start research in quantum information theory.

Many thanks go to Remik Augusiak and Jordi Tura, who played a special role in my PhD. I worked closely with them on many projects, and they have both taught me a lot about quantum information. I greatly appreciated their mentorship, and I will miss the fun and humour that always accompanied our collaborations.

I would like to further acknowledge my co-authors, namely Flavio Baccari, Boris Bourdoncle, Joe Bowles, Jed Kaniewski, Ivan Šupić, Peter Wittek, Erik Woodhead, as well as all of my co-authors from the experimental paper, in particular Stefano Paesani and Jianwei Wang. Many thanks to all of them for their friendliness and their hard work.

I would also like to thank everybody who is or was part of the QIT group at ICFO, for the great atmosphere at work and outside of work. Special thanks to those who were my officemates over the years, in particular Gonzalo de la Torre, Alejandro Máttar and Alex Pozas-Kerstjens. I would also like to thank my undergraduate student, Alvaro Ortega, for his enthusiasm and his hard work.

Many thanks to all the teams in management, administration and outreach at ICFO for providing me with a great environment in which to do my PhD. I am particularly grateful for all the help I received with administrative matters, travel payments, and for the opportunity to follow language classes during my stay.

During my PhD, I was able to take part in many activities. I would like to acknowledge the members of the Young PhD Students reading group: Flavio Baccari, Boris Bourdoncle, Florian Curchod, Leo Guerini, and Ivan Šupić, as well as all those who joined us during our sessions. I believe the group was extremely beneficial to me at the start of my PhD. I would also like to thank all the members of the Quantum Machine Learning reading group – in particular the founder Peter Wittek. I had the great opportunity to organise one of the editions of the YQIS conference and I would like to thank my co-organisers Boris Bourdoncle, Flavio Baccari and Alejandro Máttar, as well as the founders of YQIS, Alain Aspect and Sébastien Tanzilli, and of course our supervisor Toni for his support during this endeavour.

I also had the opportunity to travel abroad on academic visits and I am grateful to the groups of Stefano Pironio and Nicolas Cerf in Brussels, of Nicolas Brunner in Geneva, of Marcus Huber in Vienna, and of Stephanie Wehner in Delft (with special thanks to Gláucia Murta) for their warm welcome.

Concerning the thesis itself, I would like to thank Flavio Baccari, Boris Bourdoncle, Gláucia Murta, Ivan Šupić, and especially Joe Bowles for their insightful comments on the text, as well as Sarah Keary for her precious help on the day of the thesis submission. Many thanks also to Boris Papeians who designed the cover picture.

Finally, I would like to express my deepest gratitude to my dearest friends and family for their continuous love and support during the last few years.

Abstract

The technological era that we live in is sometimes described as the Information Age. Colossal amounts of data are generated every day and considerable effort is put into creating technologies to process, store and transmit information in a secure way. Quantum Information Science relies on quantum systems to develop new information technologies by exploiting the non-classical properties of those systems, such as entanglement or superposition. Quantum computing has recently received substantial investment, and quantum random number generators and cryptography systems are already available commercially.

Entanglement is one of the counter-intuitive, mysterious phenomena that quantum theory is known to describe. Two entangled particles are such that, even when they are spatially separated, their quantum state can only be described for the system as a whole, and not as two independent quantum states. This implies that when making measurements on entangled particles, particular correlations between the measurement outcomes may appear which cannot be obtained with pre-shared classical information. Such correlations, termed nonlocal, can be detected using mathematical objects called Bell inequalities, that correspond to hyperplanes in the set of correlations obtained in a so-called Bell scenario. Many Bell experiments were conducted in which violations of Bell inequalities were measured, thus confirming the existence of nonlocality in Nature.

The last decade has seen the development of a new paradigm in quantum information theory, called the device-independent paradigm. The security and success of a device-independent protocol relies on the observation of nonlocal correlations in a Bell experiment. Moreover, the nature of Bell scenarios is such that very few assumptions on the experimental apparatus are needed, hence the name device-independent. In this framework, Bell inequalities serve as certificates that guarantee properties and quantities such as the randomness of a series of numbers or the security of a secret key shared between users. It is even possible to certify which quantum state and measurements were used in the experiment based solely on the correlations they produce: this task is called self-testing.

The goal of this thesis is the study of Bell inequalities, both as fundamental objects and as tools for device-independent protocols. We consider in par-

ticular protocols for randomness certification, quantum key distribution and self-testing.

In Chapter 3, we develop robust self-testing procedures for the chained Bell inequalities, which also imply randomness certification. The chained Bell inequalities are a family of Bell inequalities that are relevant for a scenario with an arbitrary number of measurement choices. In Chapter 4, we introduce a family of Bell inequalities maximally violated by the maximally entangled states, valid for a scenario with any number of measurement choices as well as any number of measurement outcomes. We study the properties of these Bell inequalities in depth, and discuss through examples their applications to self-testing, randomness certification and quantum key distribution. We also present an extension of our results to any number of parties, as well as experimental results obtained in an international collaboration, where we measure violations of our Bell inequalities for local dimension up to 15. In Chapter 5, we consider the question of randomness certification from partially entangled states. We show, through self-testing results, that maximal randomness can be certified from any partially entangled state of two qubits, using the Clauser-Horne-Shimony-Holt inequality and its tilted version.

Resumen

La era tecnológica en la que vivimos en ocasiones es descrita como la Era de la Información. Todos los días se generan cantidades colosales de datos y se pone un gran esfuerzo en crear tecnologías para procesar, almacenar y transmitir esta información de manera segura. La teoría de la información cuántica se basa en los sistemas cuánticos para desarrollar nuevas tecnologías de la información mediante la explotación de sus propiedades no clásicas, tales como el entrelazamiento o la superposición. La computación cuántica ha recibido recientemente una inversión sustancial, y algunos sistemas de criptografía cuántica ya están disponibles en el mercado.

El entrelazamiento es uno de los fenómenos contraintuitivos y misteriosos descritos por la teoría cuántica. Dos partículas entrelazadas son tales que, incluso cuando están separadas espacialmente, su estado cuántico solo se puede describir como el de un sistema conjunto y no como dos estados cuánticos independientes. Esto implica que al realizar medidas sobre partículas entrelazadas, pueden aparecer correlaciones particulares entre los resultados de las medidas que no se pueden obtener con información clásica precompartida. Dichas correlaciones, denominadas no-locales, se pueden detectar utilizando objetos matemáticos llamados desigualdades de Bell. En la actualidad un gran número de experimentos de Bell han confirmado la existencia de no-localidad en la naturaleza a través de la observación de violaciones de desigualdades de Bell.

La última década ha sido testigo del desarrollo de un nuevo paradigma en la teoría de la información cuántica, llamado el paradigma *device-independent* (independiente de dispositivos). La seguridad y el éxito de un protocolo *device-independent* se basan en la observación de correlaciones no-locales en un experimento de Bell. La naturaleza de los escenarios de Bell es tal que se necesitan muy pocas suposiciones sobre la implementación experimental, de ahí el nombre *device-independent*. En este marco, las desigualdades de Bell sirven como certificados que garantizan propiedades y cantidades, como la seguridad de una clave secreta compartida entre usuarios. Incluso se puede certificar qué estado cuántico y qué medidas se utilizaron en un experimento, basándose únicamente en las correlaciones que observadas: esta tarea se denomina *self-testing* (autoevaluación).

El objetivo de esta tesis es el estudio de las desigualdades de Bell, tanto

como objetos fundamentales como como herramientas para protocolos *device-independent*. En particular, consideramos protocolos para la certificación de aleatoriedad, la distribución cuántica de claves secretas y el *self-testing*.

En el Capítulo 3, desarrollamos protocolos robustos de *self-testing* para las desigualdades de Bell encadenadas (que son relevantes para un escenario con un número arbitrario de opciones de medición), lo que también implica una certificación de aleatoriedad. En el Capítulo 4, introducimos una familia de desigualdades de Bell cuya violación máxima es obtenida con estados máximamente entrelazados, válidas para un escenario con cualquier número de opciones de medición, así como cualquier número de resultados por cada medición. Estudiamos en profundidad las propiedades de estas desigualdades de Bell y analizamos a través de ejemplos sus aplicaciones para protocolos *device-independent*. También presentamos una extensión de nuestros resultados a cualquier número de partes, así como resultados experimentales obtenidos en una colaboración internacional, donde medimos violaciones de nuestras desigualdades de Bell hasta una dimensión local de 15. En el Capítulo 5, consideramos la cuestión de la certificación de aleatoriedad a partir de estados parcialmente entrelazados. Mostramos, a través de resultados de *self-testing*, que se puede certificar una cantidad máxima de aleatoriedad a partir de cualquier estado parcialmente entrelazado de dos qubits, utilizando la desigualdad de Clauser-Horne-Shimony-Holt y su versión *tilted*.

Resum

L'era tecnològica en què vivim és a vegades descrita com l'era de la informació. Cada dia es generen quantitats colossals de dades i s'està dedicant un esforç considerable a la creació de tecnologies per processar, emmagatzemar i transmetre informació de manera segura. La teoria quàntica de la informació es fonamenta en l'ús de sistemes quàntics per tal de desenvolupar noves tecnologies de la informació que exploten les propietats no clàssiques d'aquests sistemes, com ara l'entrellaçament o la superposició. La computació quàntica ha rebut recentment inversions substancials, i criptosistemes quàntics es troben ja disponibles comercialment.

L'entrellaçament és un dels fenòmens més contra-intutius i misteriosos que descriu la teoria quàntica. Dos partícules entrellaçades són tals que, fins i tot quan es troben separades espacialment, el seu estat quàntic pot ser descrit només prenent el sistema complet com una sola entitat, i no com dos estats quàntics independents. Això implica que al mesurar partícules entrellaçades, certes correlacions entre els resultats de les mesures poden sorgir, i aquestes correlacions no es podrien obtenir només amb informació clàssica pre-compartida. Tals correlacions, denotades no-locals, es poden detectar mitjançant ens matemàtics anomenats desigualtats de Bell. Al llarg de la història, s'han fet multitud d'experiments de Bell en els quals s'ha observat la violació de desigualtats, confirmant doncs l'existència de la no-localitat en la naturalesa.

L'última dècada ha estat testimoni del desenvolupament d'un nou paradigma en la teoria quàntica de la informació, anomenat *device-independent* (independent del dispositiu). La seguretat i l'èxit d'un protocol *device-independent* es fonamenta en l'observació de correlacions no-locals en la realització d'un experiment de Bell. La naturalesa dels escenaris de Bell és tal que realment poques hipòtesis sobre el funcionament dels aparells usats durant l'experiment són necessàries, donant lloc a la nomenclatura *device-independent*. En aquest marc de treball, les desigualtats de Bell serveixen com a certificats que garanteixen les propietats i les quantitats com ara la seguretat d'una clau secreta compartida entre usuaris. És fins i tot possible certificar quins estats quàntics i mesures foren utilitzats en l'experiment, només a partir de les correlacions que produeixen. Aquesta última tasca s'anomena *self-testing* (autoavaluació).

L'objectiu d'aquesta tesi és l'estudi de les desigualtats de Bell, tant des del punt de vista fundacional, com també com a eines per a protocols *device-independent.* Considerem en particular protocols per a la certificació d'aleatorietat, distribució quàntica de claus i *self-testing.*

En el Capítol 3, desenvolupem protocols robusts de *self-testing* per a les desigualtats de Bell encadenades, els quals també impliquen la certificació de l'aleatorietat. Les desigualtats de Bell encadenades formen una família de desigualtats que són d'especial rellevància per un escenari amb un nombre arbitrari d'eleccions de mesures. En el Capítol 4, presentem una família de desigualtats de Bell que són màximalment violades per estats màximalment entrellaçats, les quals són vàlides en escenaris amb un nombre arbitrari d'eleccions de mesures així com un nombre també arbitrari de resultats per a les mesures. Estudiem les propietats d'aquestes desigualtats de Bell en profunditat, i discutim a través d'exemples les seves aplicacions als protocols *device-independent.* També presentem una extensió dels nostres resultats a un nombre de partícules arbitrari, així com resultats experimentals obtinguts en el marc d'una col·laboració internacional, en la que mesurem les violacions de les nostres desigualtats de Bell en sistemes on la dimensió local arriba fins a 15. En el Capítol 5, considerem la qüestió de la certificació de l'aleatorietat a partir d'estats parcialment entrellaçats. Demostrem, a través de resultats de *self-testing*, que l'aleatorietat màxima pot ésser certificada partint de qualsevol estat entrellaçat de dos bits quàntics, emprant la desigualtat de Clauser-Horne-Shimony-Holt i la seva versió obliqua.

List of publications

This PhD thesis is based on the following publications and preprints:

- I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, *Self-testing protocols based on the chained Bell inequalities*, New J. Phys. **18**, 035013 (2016)
- A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, *Bell inequalities tailored to maximally entangled states*, Phys. Rev. Lett. **119**, 040402 (2017)
- J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson, *Multidimensional quantum entanglement with large-scale integrated optics*, Science **360**, 285-291 (2018)
- E. Woodhead, J. Kaniewski, B. Bourdoncle, A. Salavrakos, J. Bowles, R. Augusiak, and A. Acín, *Maximal randomness from partially entangled states*, arXiv:1901.06912 (2019)

Other publications and preprints not included in this thesis:

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

Contents

List of acronyms

BKP - Barrett-Kent-Pironio
CGLMP - Collins-Gisin-Linden-Massar-Popescu
CHSH - Clauser-Horne-Shimony-Holt
DI - Device-independent
GHZ - Greenberger-Horne-Zeilinger
LHV - Local Hidden Variable
LOCC - Local Operations and Classical Communication
MMI - Multimode interfermoters
MZI - Mach-Zehnder Interferometers
NPA - Navascués-Pironio-Acín
POVM - Projective Operator Valued Measure
QKD - Quantum Key Distribution
RHOM - Reversed Hong-Ou-Mandel
SDP - Semidefinite Programme
SFWM - Spontaneous Four-Wave Mixing
SOS - Sum-of-squares

1. Objectives and main results

The advent of Quantum Information Science is sometimes referred to as the *second quantum revolution*, in the sense that quantum systems are now being used as the building blocks for new technologies. What characterises these new technologies is their ability to create, control and manipulate quantum systems individually. The *qubit*, i.e. the quantum bit, is central to quantum information science. In contrast, the first quantum revolution of the early twentieth century was about the discovery of quantum mechanics and its novel set of rules. The technologies that ensued contain quantum effects, but are based on ensembles of quantum systems instead of individual ones. Examples include lasers and transistors that have many applications in everyday life, for instance through computers and medical devices.

A property that is at the heart of many quantum information protocols is *entanglement*. With his work, John Bell put entanglement and its peculiar properties on the front of the stage and in that sense, he played a role in triggering the second quantum revolution [Asp04]. Bell inequalities establish a clear frontier between classical and quantum behaviour by providing a way to experimentally detect the distinctive correlations, termed *nonlocal*, that are produced by making measurements on entangled particles.

Bell's work came at a time when a common attitude among physicists was to take the foundations and basic concepts of quantum mechanics as given and focus on their applications instead. The 1964 article [Bel64] went mostly unnoticed for a few years, but gained fame when experimental tests of nonlocality were performed [ADR82]. The story of Bell's work shows that there is great value in investigating fundamental problems. Nowadays, there is still a significant dialogue between quantum information processing and quantum foundations – problems motivated by the former often produce results that are relevant to the latter, and vice-versa [dlT15].

Quantum information science is a young and very active field, pushed forward by the efforts of physicists, mathematicians, computer scientists and engineers. It aims at solving problems in the domain of information processing and transmission using quantum systems, thus using the rules of quantum mechanics. Subjects in quantum information science include quantum computation, cryptography, communication, quantum key distribution, random number generation, and more. Quantum computing has received a lot of attention lately, also from the general public with famous "tech" companies investing into the field such as IBM, Google and Microsoft [IBM, Goo, Mic]. Quantum cryptography is more mature as a technology, and there exist companies that manufacture quantum cryptography systems and quantum random number generators [IDQ, Qui].

A decade ago, a new paradigm started developing in quantum information theory, called the device-independent paradigm. In the device-independent paradigm, the success of information processing protocols rests on the observation of the nonlocal correlations produced by entangled states, which can be achieved by measuring the violation of a Bell inequality. The security does not require assumptions on the exact quantum state and measurements used in the protocol – it is thus not necessary to control the apparatus perfectly [BCP+14]. Self-testing is a protocol very particular to the device-independent approach: from the correlations produced by the apparatus, the goal is to certify which quantum states and measurements were in fact employed.

Bell inequalities are central to the device-independent approach. We said earlier that Bell's work played a role in triggering the second quantum revolution of the last decades, and we now observe that his work is still very much part of it. We can see Bell inequalities as having two roles in quantum information science: on the one hand, they are fundamental tools that allow for the demonstration of nonlocal correlations in Nature [HBD+15], and on the other hand they can be used as certificates in quantum information processing protocols.

This thesis is focused on device-independence, and Bell inequalities appear throughout the text, sometimes as the main subject of our study, and sometimes as the means to perform tasks such as self-testing, quantum key distribution and randomness certification.

Motivation and results

Let us introduce the themes on which we worked, the questions that triggered our research, and the contributions we were able to bring.

Chained Bell inequalities: self-testing and randomness certification

Self-testing is the task of certifying which states and measurements were used in an experiment, based on the observed correlations only. Since the introduction of self-testing in [MY04], a series of work has aimed to self-test different quantum states and measurements in various scenarios (see, e.g. [MYS12, BP15]). In particular, a procedure was recently designed to self-test all pure bipartite quantum states [CGS17].

The chained Bell inequalities were introduced in [Pea70]. They are the natural generalisation of the famous Clauser-Horne-Shimony-Holt (CHSH) Bell inequalities [CHSH69] to a scenario with an arbitrary number of measurement choices. They appear in several quantum information processing protocols, for instance in [MPA11] for quantum key distribution and in [DPA13] for randomness certification. The question of using the chained Bell inequalities for self-testing arose naturally given the existing self-tests at the time of our work. The measurements maximally violating the chained Bell inequalities are particularly interesting to self-test, especially given that measurement self-testing remains less explored than state self-testing.

Our contributions

We built a robust self-testing procedure based on the chained Bell inequalities valid for any number of measurement choices, thus showing that these inequalities are useful for self-testing. The self-test certifies that when the maximal quantum violation of the chained Bell inequalities is observed, measurements equally spaced on the X-Z plane of the Bloch sphere were performed on the maximally entangled state of two qubits. This means that our procedure allows for the self-test of the whole X-Z plane of the Bloch sphere, in the limit of an arbitrarily high number of measurements. We also studied the applications of our result to randomness certification. In particular, our self-test completes the proof of [DPA13] for the certification of two random bits from the maximally entangled state of two qubits.

Bell inequalities tailored to maximally entangled states

The CHSH Bell expression possesses several attractive properties. Indeed, it is tight (it corresponds to a facet of the polytope of classical correlations [BCP+14]), and its maximal quantum violation is obtained by a maximally entangled state on which mutually unbiased measurements [DEBZ10] are made. The CHSH expression is designed for the simplest Bell scenario, i.e. for two parties that have two measurements choices with two outcomes each. When constructing Bell inequalities for more complicated scenarios, it turns out to be very difficult to keep all of those properties in one Bell expression. For instance, the Collins-Gisin-Linden-Massar-Popescu (CGLMP) Bell inequalities [CGL+02] generalise CHSH to many measurement outcomes, and are maximally violated by *partially* entangled states [ADGL02, ZG08]. This result was a surprise at the time it was found, and was even thought of as an anomaly in the relation between nonlocality and entanglement.

However, let us note that the CGLMP Bell inequalities were constructed with the aim of nonlocality detection in mind, and techniques related to the set of classical correlations were used. This means that we should not necessarily be surprised that they do not conserve the quantum properties of CHSH. On the other hand, they conserve the "classical" properties of CHSH, as they are facets of the local polytope and have good noise resistance. Our goal was to find generalisations of the CHSH inequality maximally violated by maximally entangled states – since this is a quantum property, we used a method based on a quantum framework.

Our contributions

We obtained a family of Bell inequalities valid for any number of measurement choices and measurement outcomes that is maximally violated by the maximally entangled state of two qudits. We studied the properties of this family of inequalities and obtained analytical expressions for their different bounds. We also discussed their applications to device-independent protocols, in particular we performed self-testing of the maximally entangled two-qutrit state, using a numerical method introduced in [YVB$^+$14]. Then, we were able to generalise most of our findings to any number of parties. We also considered a modification of our inequalities in the particular case of two measurement choices and three measurement outcomes, where we obtain a family of Bell inequalities maximally violated by a family of partially entangled states – by changing a parameter in the Bell expression, one changes the optimal state. Finally, we had the opportunity to be part of an international collaboration led by the Quantum Photonics group of the University of Bristol, UK, that developed a quantum "chip" capable of generating and manipulating entangled bipartite qudit states up to local dimension 15. Together, we were able to observe violations of our Bell inequalities and perform self-testing and randomness certification.

Randomness from partially entangled states

Generating random numbers from the intrinsic randomness of quantum mechanics is arguably one of the most attractive ideas in quantum information theory. Pironio *et al.* showed that this task could be done in a device-independent way in their work based on the CHSH Bell inequality [PAM$^+$10]. In this framework, an interesting question arises about the relation between randomness and entanglement. As a first guess, it is natural to think that randomness is a monotonous function of entanglement, where maximal randomness could only be obtained when measuring maximally entangled states. This intuition was proven wrong in [AMP12], where the authors showed that one bit of local randomness (i.e. when looking at the output of one user only) can be certified from any partially entangled state of two qubits. When considering global randomness (i.e. when looking at the outputs of both users), while two random bits can be certified from the maximally entangled state [DPA13], the authors of [AMP12] showed that arbitrarily close to this same quantity can be certified from states with arbitrarily small entanglement. The case of reaching exactly two random bits with all partially entangled states between these two extremal cases was left as an open question, which we investigated.

Our contributions

We were able to show that two bits of global randomness can be certified from *all* partially entangled state of two qubits. We followed two different approaches to answer this question, and present both in this thesis. In the first one, we based our work on a combination of two tilted CHSH inequalities from [AMP12] and one CHSH inequality. The main challenge is that all three directions X, Y, and Z of the Bloch sphere are used for this task, contrarily to the case of maximally entangled states where a plane of the Bloch sphere suffices. We also considered the question of local randomness certification using positive-operator valued measurements (POVMs). In our second approach, we modified the Elegant Bell inequality introduced in [Gis09] to obtain a tilted version optimal for partially entangled states. Our second approach uses fewer measurement choices than the first one, but works only for a range of partially entangled states.

Outline of the thesis

This thesis is organised as follows:

- Chapter 2 reviews the basic concepts and tools that are then used throughout the thesis.

- Chapter 3 is devoted to the self-testing protocols that can be developed based on the chained Bell inequalities and their applications to randomness certification. The chapter is based on [ŠASA16].

- Chapter 4 is dedicated to the construction and study of a family Bell inequalities for maximally entangled states. Sections 4.1, 4.3 and 4.4 are based on [SAT$^+$17] and [WPD$^+$18]. Section 4.2 contains material to be published, which is the result of a collaboration with Jordi Tura and Remigiusz Augusiak.

- Chapter 5 studies how randomness can be certified from partially entangled states of two qubits. Section 5.1 is based on [WKB+19] and Section 5.2 contains material to be published, which was obtained in collaboration with Erik Woodhead, Boris Bourdoncle and Antonio Acín.

2. Background

In this chapter, we introduce the concepts and tools that will be used in the remainder of this thesis. We review the definitions of entanglement, nonlocality and Bell inequalities, as well as methods for the characterisation of quantum correlations. This leads us to the paradigm of device-independence, where the success of information protocols is based on the violation of Bell inequalities, which are central to this thesis. Expert readers may skip this chapter.

2.1. Entanglement

Entanglement has been a key concept of quantum physics for more than 80 years - it was first used by Schrödinger following the publication of the famous EPR paper in 1935 [EPR35]. The notion of entanglement captures the characteristic of a composite system that cannot be thought of as two (or more) separated subsytems - it has no classical counterpart and is considered to be one of the "spooky" or counterintuitive features of quantum physics.

Formally, if we consider a system made of N subsystems described by a state ρ acting on a Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_N$, it is said that ρ is *separable* if it can be written as a convex combination of product states, i.e.

$$\rho = \sum_\lambda p_\lambda \rho_1^\lambda \otimes \rho_2^\lambda \otimes \ldots \otimes \rho_N^\lambda, \tag{2.1}$$

where ρ_i acting on $\mathcal{H}_i$ is the quantum state of the ith subsystem, and all p_λ coefficients are non-negative $p_\lambda \geq 0$ and sum to one $\sum_\lambda p_\lambda = 1$. If ρ cannot be written as (2.1), then it is *entangled.*

An important feature of multi-particle entanglement is genuine multipartite entanglement [GT09, BGLP11]. A quantum state is said to be *genuine multipartite entangled* when it cannot be decomposed as a convex combination of biseparable states (states which are separable on at least one bipartition of the parties). For example, in the case of three parties, a state ρ_{bisep} is said to be *biseparable* if it admits the convex decomposition:

$$\rho_{\text{bisep}} = \sum_\lambda p_\lambda^{12|3} \rho_{1,2}^\lambda \otimes \rho_3^\lambda + \sum_\lambda p_\lambda^{13|2} \rho_{1,3}^\lambda \otimes \rho_2^\lambda + \sum_\lambda p_\lambda^{23|1} \rho_{2,3}^\lambda \otimes \rho_1^\lambda, \tag{2.2}$$

where the indices $1, 2, 3$ denote the party or particle, and all coefficients are non-negative $p_\lambda^{ij|k} \geq 0$ and $\sum_\lambda p_\lambda^{12|3} + p_\lambda^{13|2} + p_\lambda^{23|1} = 1$. A state that cannot be decomposed as (2.2) is genuine tripartite entangled.

There exist several entanglement measures to quantify the entanglement present in a system. In the simplest case of pure bipartite states, the *maximally entangled state* is defined as:

$$|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle. \tag{2.3}$$

It is the only state that can be transformed deterministically to any other by local operations assisted by classical communication (LOCC), and at the same time, cannot be obtained from any other deterministically. For multipartite states, there is no such state. Nevertheless, sets or classes of entanglement can be defined (see for instance [dVSK13]), and different entanglement measures will define different maximally entangled states [SSC+15]. Such a family of multipartite states that are defined as maximally entangled according to several measures are the Greenberger-Horne-Zeilinger (GHZ) states [GHZ89]. For three parties the GHZ state simply reads: $|\mathrm{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$. For N parties and d dimensions, we consider the generalised GHZ state:

$$|\mathrm{GHZ}_{N,d}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii \ldots i\rangle. \tag{2.4}$$

The GHZ state is genuine multipartite entangled.

2.2. Nonlocality

Making measurements on entangled particles can yield very particular correlations that cannot be explained classically. In 1964, a few decades after EPR, John Bell designed a thought experiment to highlight this phenomenon called nonlocality [Bel64]. The setup is often called *Bell scenario* or *Bell experiment* [BCP+14].

2.2.1. Bell experiments and sets of correlations

In a Bell experiment, two parties A and B (often called Alice and Bob) receive a share of a physical system from a source, on which they make measurements, as pictured in Figure 2.1. To this end, they introduce inputs $x, y \in \{1, \ldots, m\}$ into their devices, and receive outputs $a, b \in \{0, \ldots, d-1\}$, respectively. For

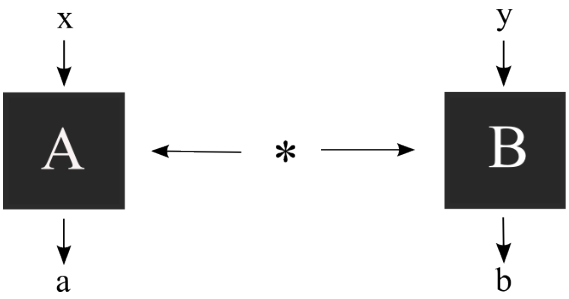

Figure 2.1.: A bipartite Bell experiment. A source sends physical systems to parties A and B, who perform measurements on their share of the systems. To this end, they introduce inputs x and y in their devices, which can be seen as black boxes, and receive ouputs a and b.

the Bell test to be valid, two assumptions must be respected: the parties cannot communicate with each other (which can be enforced by making their measurements spacelike separated events), and their inputs cannot be correlated to the apparatus (which can be enforced by choosing them at random). There are no further requirements on the users' devices, which can be considered as *black boxes*.

By repeating these measurements a large number of times, the users can collect the statistics and estimate the conditional probabilities $P(a,b|x,y)$ that Alice and Bob obtain outcomes a and b upon performing the xth and yth measurement, respectively. These probabilities are ordered into a vector, sometimes called a *behaviour*:

$$\vec{p} := \{P(a,b|x,y)\}_{a,b,x,y} \in \mathbb{R}^{(md)^2}. \tag{2.5}$$

Importantly, the set of allowed vectors $\vec{p}$ varies depending on the physical theory they obey, and different principles lead to different sets of correlations in $\mathbb{R}^{(md)^2}$, as pictured in Figure 2.2.

If the Bell experiment is well defined and Alice and Bob cannot communicate with each other, the observed correlations should obey the *no-signalling principle*. Mathematically :

$$\begin{aligned} \sum_{b=0}^{d-1} P(ab|xy) &= \sum_{b=0}^{d-1} P(ab|xy') \qquad \forall a,x,y,y' \\ \sum_{a=0}^{d-1} P(ab|xy) &= \sum_{a=0}^{d-1} P(ab|x'y) \qquad \forall b,x,x',y. \end{aligned} \tag{2.6}$$

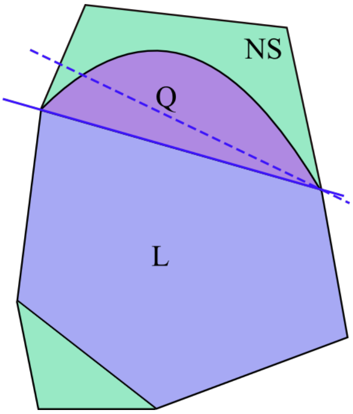

Figure 2.2.: Representation of the sets of correlations $\vec{p} \in \mathbb{R}^{(md)^2}$ obtained from a Bell experiment. The local set $\mathcal{L}$ as well as the no-signalling set $\mathcal{NS}$ are convex polytopes, and the quantum set $\mathcal{Q}$ is simply convex. Bell inequalities are hyperplanes: the continuous line represents a facet Bell inequality, and the dashed line a tilted Bell inequality.

This means that $P(a|x) = P(a|xy) = P(a|xy')$, i.e. Alice's local marginal probabilites are independent of Bob's input choice, and vice-versa. These correlations form a convex polytope denoted $\mathcal{NS}$ [PR94].

Contained in this set is the set of *quantum* correlations $\mathcal{Q}$, i.e. those obtained by performing measurements on a quantum state, according to the Born rule. It is formed by those $\vec{p}$ whose components can be written as

$$P(ab|xy) = \text{tr}\ (\rho_{AB} M_{a|x} \otimes N_{b|y}), \tag{2.7}$$

where ρ_{AB} is a quantum state acting on a joint Hilbert space $H_A \otimes H_B$ of unconstrained dimension, and $M_{a|x}$ and $N_{b|y}$ are measurement operators defining, respectively, Alice's and Bob's measurements. $M_{a|x}$ denotes the operator yielding outcome a given a measurement choice x on system A, and $N_{b|y}$ denotes the operator yielding outcome b given a measurement choice y on system B.

In general, the measurement operators are *positive-operator valued measure* (POVM) elements satisfying $M_{a|x} \geq 0$ and $\sum_{a=0}^{d-1} M_{a|x} = \mathbb{I}$, and similarly for Bob's operators. We can however assume that the measurement operators are orthogonal projectors, by increasing the dimension of the Hilbert space [NC11]. Their properties are then $M_{a|x}M_{a'|x} = \delta_{aa'}M_{a|x}$ and $\sum_{a=0}^{d-1} M_{a|x} = \mathbb{I}$, and similarly for Bob's operators. Note that from the projection operators we can build *observables* $M = \sum_{a=0} m_a M_{a|x}$, with m_a the eigenvalue associated to projector $M_{a|x}$. Observables are usually defined as Hermitian, with real eigenvalues m_a (often chosen as -1 and $+1$ when $d = 2$). It is not always the case in many-outcome scenarios, as we will see in Chapter 4 where we define unitary but non-Hermitian observables with complex eigenvalues.

By increasing the dimension of the Hilbert space, it is also possible to purify the state ρ_{AB} to a state $|\psi\rangle_{AB}$ so that the Born rule becomes $P(ab|xy) = \langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle$.

Finally, if the Bell experiment can be explained by a local hidden variable (LHV) model, $\vec{p}$ is said to be *local* and its elements can be written as

$$P(ab|xy) = \int_{\Lambda} d\lambda q(\lambda) D(a|x, \lambda) D(b|y, \lambda), \tag{2.8}$$

where the variables λ belong to a space Λ and $q(\lambda)$ is their probability distribution. Here $D(a|x, \lambda)$ and $D(b|y, \lambda)$ are the local probability response functions for Alice and Bob. They are denoted D as they can be taken to be deterministic [Fin82], which means that they take values 0 or 1. This definition expresses that the local outcomes of Alice and Bob can be fully explained by hidden variables λ and their input x and y respectively, excluding any “influence” exerted by the other party's measurement. The local set $\mathcal{L}$ is a convex polytope.

Bell was the first to prove that not all quantum correlations admit an LHV model, which establishes that $\mathcal{L} \subset \mathcal{Q}$. Also, there exist correlations that respect the no-signalling principle but that are not quantum, such as the PR-box [PR94]. This means that $\mathcal{Q} \subset \mathcal{NS}$. Correlations that do not belong to $\mathcal{L}$, i.e. cannot be written as (2.8) are called *nonlocal*.

2.2.2. Bell inequalities

Since $\mathcal{L}$ is a convex polytope, for each nonlocal behaviour $\vec{p}$ there exists a hyperplane separating it from $\mathcal{L}$. Those hyperplanes correspond to *Bell inequalities* [Fro81]. A Bell expression I is defined as a linear combination of the $(md)^2$ joint probabilities:

$$I = \sum_{abxy} k_{abxy} P(ab|xy), \tag{2.9}$$

where the coefficients k_{abxy} are real numbers. It is sometimes more practical to express Bell inequalities in terms of *correlators* or expectation values $\langle A_x B_y\rangle$ of Alice and Bob's observables for measurements x and y, respectively. Definitions of $\langle A_x B_y\rangle$ may vary according to the problem considered (see for instance Chapter 4), but in general we have:

$$\langle A_x B_y\rangle = \sum_{a,b} ab P(ab|xy). \tag{2.10}$$

A Bell inequality $I \leq \beta_C$ must be satisfied by all local correlations, where $\beta_C = \max_{\vec{p} \in \mathcal{L}} I$ is the *classical bound*, i.e. the maximum value of I achieved by local probability distributions. The *quantum* or *Tsirelson bound* of I is the maximum value $\beta_Q = \max_{\vec{p} \in \mathcal{Q}} I$ of the Bell expression for quantum behaviours [Cir80]. A Bell expression I gives rise to a non-trivial Bell inequality, i.e. one that is violated by quantum theory, if $\beta_C < \beta_Q$. Finally, one defines the *no-signalling bound* $\beta_{NS} = \max_{\vec{p} \in \mathcal{NS}} I$ as the maximum value of I over no-signalling correlations. For most of the Bell inequalities that have been studied, $\beta_{NS} > \beta_Q > \beta_C$ [Bel64, PR94, RTHH16].

As shown in Figure 2.2, Bell inequalities can correspond to facets of the local polytope, which are faces of dimension $\dim(\mathcal{L}) - 1$. They are then called *facet* or *tight* Bell inequalities. However, it is not necessary for Bell inequalities to be facets. In the case where the coefficients of a Bell expression are modified such that the resulting Bell inequality ceases to be tight, we refer to it as a *tilted* Bell inequality.

2.2.3. Characterisation of quantum correlations and semidefinite programming

The sets $\mathcal{L}$ and $\mathcal{NS}$ are polytopes, and can thus be described by a finite number of extreme points or a finite number of linear inequalities. Deciding whether a behaviour belongs to $\mathcal{L}$ or to $\mathcal{NS}$ thus amounts to finding all those vertices or inequalities. Since $\mathcal{Q}$ is not a polytope, there is no such closed formulation to determine whether a behaviour is quantum. How can we answer the question: given a point $\vec{p}$, do there exist a state ρ_{AB} and measurements $M_{a|x}$ and $N_{b|y}$ that yield $\vec{p}$ through the Born rule?

This is a question that influences both foundations of quantum mechanics and practical applications of nonlocality. On the fundamental side, there have been attempts to characterise $\mathcal{Q}$ analytically, in particular to find information principles which would allow to recover $\mathcal{Q}$ “from scratch” [PPK+09, NW10, FSA+13, NGHA15]. In the remainder of this thesis, we will encounter several examples of how the characterisation of $\mathcal{Q}$ is of practical interest in quantum information protocols.

The Navascués-Pironio-Acín hierarchy

Navascués, Pironio and Acín introduced a hierarchy (often called the NPA hierarchy) of necessary conditions that a quantum behaviour $\vec{p} \in \mathcal{Q}$ must satisfy [NPA07, NPA08]. Whenever correlations do not satisfy a condition of this hierarchy, we can conclude that they lie outside the quantum set.

Let us start from a behaviour $\vec{p} = \{P(a,b|x,y)\}_{a,b,x,y}$ satisfying equation (2.7). This means there exist a state ρ_{AB} and measurement operators $M_{a|x}$, $N_{b|y}$ (that we can take to be projectors since the dimension of the Hilbert space is not constrained) that yield this behaviour. Instead of specifically ensuring the product structure $M_{a|x} \otimes N_{b|y}$, one can simply consider operators $\tilde{M}_{a|x} = M_{a|x} \otimes \mathbb{I}$ and $\tilde{N}_{b|y} = \mathbb{I} \otimes N_{b|y}$ with the condition that these new operators on Alice and Bob's side should commute with each other $[\tilde{M}_{a|x}, \tilde{N}_{b|y}] = 0$. This implies a first *relaxation* of the problem which defines a new set $\mathcal{Q}^{\text{comm}}$ that contains the quantum set $\mathcal{Q} \subseteq \mathcal{Q}^{\text{comm}}$.

We can build a set $\mathcal{S} = \{S_1, \dots S_k\}$ made of k different combinations of operators $\tilde{M}_{a|x}$, $\tilde{N}_{b|y}$. For a given set $\mathcal{S}$, a matrix Γ of size $k \times k$ can be constructed, such that its elements are

$$\Gamma_{ij} = \operatorname{tr}\left(S_i^\dagger S_j \rho\right). \tag{2.11}$$

This matrix is Hermitian, positive semidefinite

$$\Gamma \succeq 0, \tag{2.12}$$

and must satisfy the following linear constraints (which reflect the properties of operators $\tilde{M}_{a|x}$ and $\tilde{N}_{b|y}$, for instance that $\tilde{M}_{a|x}\tilde{M}_{a'|x} = \delta_{aa'}\tilde{M}_{a|x}$, or the commutation between Alice and Bob's operators):

$$\begin{aligned} &\sum_{i,j} c_{ij}\Gamma_{ij} = 0 \qquad \text{if} \sum_{i,j} c_{ij} S_i^\dagger S_j = 0, \\ &\sum_{i,j} c_{ij}\Gamma_{ij} = \sum_{ax,by} d_{ax,by} P(ab|xy) \qquad \text{if} \sum_{i,j} c_{ij} S_i^\dagger S_j = \sum_{ax,by} d_{ax,by} M_{a|x} N_{b|y}. \end{aligned} \tag{2.13}$$

These are the necessary conditions that form the NPA hierarchy: for a quantum behaviour $\vec{p}$, there always exists for each set $\mathcal{S}$ a matrix Γ satisfying the constraints above. This matrix is often called the *moment matrix*. For a given $\vec{p}$ and set $\mathcal{S}$, if no such matrix can be found, then $\vec{p}$ does not belong to $\mathcal{Q}$. The hierarchical structure resides in the choice of the set $\mathcal{S}$. The first *level* of this hierarchy means taking $\mathcal{S}^{(1)} = \{M_{a|x}\} \cup \{N_{b|y}\}$, the set of projectors of Alice and Bob. In general, we can define $\mathcal{S}^{(k)}$ as the set of products of at most k operators. This yields an infinity of conditions, and the hierarchy is complete: a behaviour $\vec{p}$ satisfies every condition in the hierarchy if and only if it admits a quantum representation. Note that a test performed at a given level is at least as good as the previous ones.

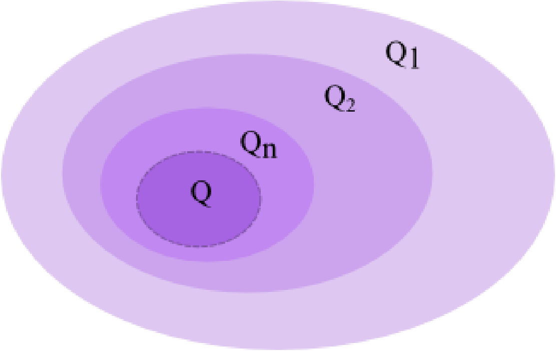

Figure 2.3.: Representation of the sets $\mathcal{Q}_k$ of the NPA hierarchy in $\mathbb{R}^{(md)^2}$ that approximate the quantum set $\mathcal{Q}$.

As pictured in Figure 2.3, each condition in the hierarchy defines a set $\mathcal{Q}_k$ in $\mathbb{R}^{(md)^2}$ of all the behaviours compatible with the existence of the matrix Γ at level k. We have that $\mathcal{Q}_1 \supseteq \mathcal{Q}_2 \supseteq \cdots \supseteq \mathcal{Q}_k \cdots \supseteq \mathcal{Q}$. Each set $\mathcal{Q}_k$ approximates $\mathcal{Q}$ better than the previous one, and the hierarchy converges to the quantum set[1].

Semidefinite programming

What makes the NPA hierarchy particularly interesting is that the question of whether a behaviour $\vec{p}$ belongs to a set $\mathcal{Q}_k$ is in fact a *semidefinite programme* (SDP). Semidefinite programming is a particular case of convex optimization, and has the following standard form [BV04]:

$$\begin{aligned} &\text{minimize} && \operatorname{tr}(CX) \\ &\text{subject to} && \operatorname{tr}(A_i X) = b_i \qquad i = 1, ..., p \\ &&& X \succeq 0. \end{aligned} \tag{2.14}$$

Here, $X, C, A_1, ...A_p$ are all Hermitian $n \times n$ matrices. The name "semidefinite program" comes from the constraint that the matrix X must be positive semidefinite. The other constraints are linear. Membership to $\mathcal{Q}_k$ indeed matches the problem (2.14), as conditions (2.13) are linear, and condition (2.12) is characteristic of semidefinite programming.

Coincidentally, there exist several methods and algorithms to solve SDPs efficiently. Many problems involving the characterisation of quantum correl-

[1] Strictly speaking, $\mathcal{Q}_{k\to\infty} \to \mathcal{Q}^{\text{comm}}$ and it remains an open question whether $\mathcal{Q}^{\text{comm}}$ and $\mathcal{Q}$ are the same [Tsi93].

ations have thus been solved numerically through the NPA hierarchy. When solving such problems in this thesis, we used programming languages Matlab (with Yalmip toolbox [Lof04] and solvers Sedumi [SA18] and Mosek [ApS17]) and Python 3 (with Picos API [Pic18] and solver Mosek [ApS18], as well as the Ncpol2sdpa library [Wit15]).

An example: the Tsirelson bound of a Bell inequality

One of the main applications of the NPA hierarchy consists in finding the quantum or Tsirelson bound of a Bell inequality. Deriving this bound is a hard task and was achieved analytically only for a few cases, since given a Bell inequality, there is no procedure that guarantees finding its quantum bound. Fortunately, using the NPA hierarchy, one can find upper bounds to β_Q of a given Bell expression I:

$$\begin{aligned} \beta_{Q_k} = \quad & \max_{\vec{p}} \quad I \\ & \text{s.t.} \quad \vec{p} \in \mathcal{Q}_k. \end{aligned} \tag{2.15}$$

According to the level of the hierarchy used, we talk about upper bound β_{Q_k} of level k. If the set $\mathcal{Q}_k$ coincides with $\mathcal{Q}$ at the point $\vec{p}$ considered, then the obtained upper bound will be tight $\beta_Q = \beta_{Q_k}$. In practice, it is often the case that the Tsirelson bound is found at a finite level, up to numerical precision.

Let us illustrate with a practical example, the Clauser-Horne-Shimony-Holt (CHSH) inequality [CHSH69]:

$$I_{CHSH} = \langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle \leq 2. \tag{2.16}$$

This Bell inequality is often written using observables and correlators, thus we keep this notation for simplicity (naturally, the problem can also be formulated with projectors and probabilities). The correlators are here defined taking $a, b \in \{-1, +1\}$:

$$\langle A_x B_y \rangle = \sum_{ab} ab P(ab|xy). \tag{2.17}$$

In the particular case of CHSH, level 1 of the hierarchy is sufficient to obtain the quantum bound $2\sqrt{2}$, which was previously obtained analytically in [Cir80]. Level 1 means choosing $\mathcal{S} = \{\mathbb{I}, A_1, A_2, B_1, B_2\}$, and Γ is a 5×5 matrix whose entries are defined by expression (2.11):

$$\begin{pmatrix} \mathrm{tr}\,(\mathbb{I}\rho) & \mathrm{tr}\,(A_1\rho) & \mathrm{tr}\,(A_2\rho) & \mathrm{tr}\,(B_1\rho) & \mathrm{tr}\,(B_2\rho) \\ \mathrm{tr}\,(A_1\rho) & \mathrm{tr}\,(\mathbb{I}\rho) & \mathrm{tr}\,(A_1A_2\rho) & \mathrm{tr}\,(A_1B_1\rho) & \mathrm{tr}\,(A_1B_2\rho) \\ \mathrm{tr}\,(A_2\rho) & \mathrm{tr}\,(A_2A_1\rho) & \mathrm{tr}\,(\mathbb{I}\rho) & \mathrm{tr}\,(A_2B_1\rho) & \mathrm{tr}\,(A_2B_2\rho) \\ \mathrm{tr}\,(B_1\rho) & \mathrm{tr}\,(B_1A_1\rho) & \mathrm{tr}\,(B_1A_2\rho) & \mathrm{tr}\,(\mathbb{I}\rho) & \mathrm{tr}\,(B_1B_2\rho) \\ \mathrm{tr}\,(B_2\rho) & \mathrm{tr}\,(B_2A_1\rho) & \mathrm{tr}\,(B_2A_2\rho) & \mathrm{tr}\,(B_2B_1\rho) & \mathrm{tr}\,(\mathbb{I}\rho)\,. \end{pmatrix} \tag{2.18}$$

We simplified the expression above, using the hermiticity of observables $A_i = A_i^\dagger$ and $B_i = B_i^\dagger$, and their unitarity $A_i^2 = B_i^2 = \mathbb{I}$. Problem (2.15) thus becomes:

$$\begin{aligned} \max \quad & \Gamma_{2,4} + \Gamma_{2,5} + \Gamma_{3,4} - \Gamma_{3,5} \\ \text{s.t.} \quad & \Gamma_{5\times 5} \succeq 0, \\ & \Gamma_{ii} = 1 \quad \text{for} \quad i = 1, \ldots 5, \end{aligned} \tag{2.19}$$

and yields $\beta_{Q_1} = 2\sqrt{2} = \beta_Q$.

Tsirelson bounds and sum-of-squares decompositions

To conclude this section on quantum correlations, let us present a technique to prove the quantum bound of a Bell inequality analytically. This technique exploits the *sum-of-squares* (SOS) decompositions of operators, as explored in [BP15].

For a positive semidefinite operator $\mathcal{O}$, an SOS decomposition is a finite collection of operators P_λ such that

$$\mathcal{O} = \sum_\lambda P_\lambda^\dagger P_\lambda. \tag{2.20}$$

When considering quantum behaviours, Bell expressions can be written as *Bell operators*. Bell expression $\sum_{abxy} k_{abxy} P(ab|xy)$ translates straightforwardly to its corresponding Bell operator $\mathcal{B} = \sum_{abxy} k_{abxy} M_{a|x} \otimes N_{b|y}$, where $M_{a|x}$ and $N_{b|y}$ are the measurement operators of Alice and Bob as in (2.7). For the discussed purpose, the goal is to find SOS decomposition of shifted Bell operators $\tilde{\mathcal{B}} = \beta_Q \mathbb{I} - \mathcal{B}$, where $\mathcal{B}$ is the Bell operator and β_Q is the quantum bound of the corresponding Bell expression. We expect that the operators P_λ will be polynomials of Alice and Bob's operators, and we say that the SOS decomposition is of order k if these polynomials are at most of degree k. If $\tilde{\mathcal{B}}$ can be written as (2.20) it must be semidefinite positive, which proves that β_Q provides an upper bound to the Bell expression. Indeed, if $\tilde{\mathcal{B}} \succeq 0$, then $\langle\psi|\tilde{\mathcal{B}}|\psi\rangle \geq 0$ for any state $|\psi\rangle$, which means that:

$$\langle\psi|\mathcal{B}|\psi\rangle \leq \beta_Q. \tag{2.21}$$

To show that the bound is tight and is thus the Tsirelson bound, one needs only to supply a quantum realisation of that value.

2.2.4. Extension to the multipartite case

For simplicity, we have considered the case of only two parties so far, Alice and Bob. In most of this thesis, the studied Bell scenarios are bipartite, except in Chapter 4, where some of our results are extended to the *multipartite* case.

All the concepts introduced in the previous subsections can be generalised to many parties. Denoting a_i the outcome of the ith party, and x_i its input, the behaviour resulting from an N-partite Bell experiment is:

$$\vec{p} = \{P(a_1, \ldots, a_N | x_1, \ldots, x_N)\}_{a_1,\ldots,a_N;x_1,\ldots,x_N} \in \mathbb{R}^{(md)^N}. \tag{2.22}$$

The no-signalling constraints become:

$$\begin{aligned}&\sum_{a_i} P(a_1, \ldots, a_i, \ldots, a_N | x_1, \ldots, x_i, \ldots, x_N) = \\ &\sum_{a_i} P(a_1, \ldots, a_i, \ldots, a_N | x_1, \ldots, x_i', \ldots, x_N),\end{aligned} \tag{2.23}$$

for all x_i, x_i' and $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_N$ and $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_N$ and all i. Quantum correlations are defined as:

$$P(\vec{a}|\vec{x}) = \operatorname{tr}\left(\rho_N (M_{x_1}^{a_1} \otimes \ldots \otimes M_{x_N}^{a_N})\right) \tag{2.24}$$

for an N-partite quantum state ρ_N of generally unconstrained dimension and measurement operators $M_{x_i}^{a_i}$ that define the measurement x_i performed by the ith party. Finally, correlations admitting an LHV model can be written as:

$$P(\vec{a}|\vec{x}) = \int_\Lambda d\lambda q(\lambda) P(a_1|x_1, \lambda) \ldots P(a_N|x_N, \lambda). \tag{2.25}$$

The sets in $\mathbb{R}^{(md)^N}$ retain their properties: they are all convex, and $\mathcal{L}$ and $\mathcal{NS}$ are polytopes. The structure of multipartite correlations is however richer: when $N > 2$, another set can be considered, consisting of correlations admitting a hybrid local-nonlocal model. This means that across all bipartitions of the parties, nonlocal correlations are allowed between the bipartitions, while inside a bipartition the correlations are local. For three parties, this is written as:

$$P(a_1 a_2 a_3 | x_1 x_2 x_3) = \sum_{k=1}^{3} r_k \int_\Lambda d\lambda q_{A_i A_j | A_k}(\lambda) P(a_i a_j | x_i x_j \lambda) P(a_k | x_k \lambda), \tag{2.26}$$

where $\{i, j\} \cup \{k\} = \{1, 2, 3\}$ and $r_k \geq 0$, $\sum r_k = 1$. Correlations that cannot be written in this way are called *genuine multipartite nonlocal.* For Bell inequalities, this defines an additional bound, which we call Svetlichny bound β_S [Sve87], and we have that $\beta_C \leq \beta_S$. The concepts of genuine multipartite nonlocality and genuine multipartite entanglement (see expression (2.2)) are connected, in the sense that genuine multipartite entanglement is a necessary (but not sufficient) condition to obtain genuine multipartite nonlocal correlations, in the same way that entanglement is a necessary condition for nonlocality. Hence, Svetlichny inequalities are detectors of genuine multipartite entanglement.

2.2.5. Experimental verifications

Since John Bell's paper, nonlocality has been verified experimentally by a series of experiments, starting in 1972 with Freedman and Clauser's observation of the violation of the CHSH inequality [FC72]. The experiment of Aspect and coworkers in 1982 [ADR82] is often considered to be the first one to convincingly demonstrate the existence of nonlocality. The biggest challenge in conducting experimental Bell tests is the presence of *loopholes*, i.e. defects in the experiment that allow for an LHV model to explain the violation of a Bell inequality. The main ones are the detection efficiency, locality, and finite statistics loopholes [BCP+14]. In 2015, three separate teams [HBD+15, GVW+15, SMSC+15] were able to perform the first loophole-free Bell tests.

2.3. Device-independent protocols

The last decade has seen the development of a new approach for quantum information protocols. This approach is based on Bell experiments, and is called *device-independent* (DI).

2.3.1. The device-independent paradigm

The DI paradigm is motivated by the reduced number of assumptions in a Bell scenario. The success of DI protocols rests on the observation of nonlocal correlations, i.e. on the violation of a Bell inequality, and their validity depends only on the few assumptions needed for the description of a Bell experiment (see Section 2.2.1). Thus, the internal functioning of the users' devices does not need to be specified – they are just seen as "black boxes" producing a classical output, given a classical input [BCP+14].

This makes the DI approach particularly interesting in a cryptographic context, as security can still be proven even if the devices are not fully trusted. It allows for imperfections in the implementation, contrarily to other quantum based protocols in which the exact states and measurements are described, which requires perfect experimental control.

The emergence of the DI paradigm has given a new role to nonlocality: it is now a resource or certificate for quantum information processing, and not only a foundational topic. Successful applications include DI randomness certification, DI quantum key distribution, and self-testing, which we expose in the remainder of this section.

2.3.2. Randomness certification

Motivation

Random numbers are necessary for numerous and diverse applications, ranging from cryptography and statistics to gambling and gaming [Rol15, Gen03, Gam]. There exist several approaches to generate random numbers. If the generation is based on algorithms, then the numbers produced are called pseudorandom since the process is deterministic [MN98]. Other generators are based on physical phenomena, such as thermal noise in a resistor or atmospheric noise. Ultimately, these phenomena also have a classical, i.e. deterministic explanation, hence the numbers obtained are not "truly" random. A solution presents itself in the results of quantum measurements, which contain intrinsic randomness. Various quantum schemes were developed based on, for instance, the process of splitting a beam of photons on a beamsplitter [JAW+00], and quantum random number generators are now available commercially [IDQ].

It turns out that randomness can also be *certified* using quantum systems. The certification of random numbers is a difficult question: one cannot unambiguously determine if a device is producing a random output just by looking at this output. Statistical tests of randomness have been built for this purpose, and the random numbers produced via many of the above mentioned methods pass those tests. However, with nonlocality-based protocols, the certification rests on the laws of quantum mechanics.

The intuition is the following: in a Bell scenario, the violation of a Bell inequality implies that there must be some randomness in the outputs of the experiment, and it turns out this amount of randomness can be quantified as a function of the Bell inequality violation. The idea of nonlocality-based randomness was first introduced by Colbeck in his PhD thesis supervised by Kent [Col06, CK11] and was then formalised and quantified by Pironio *et al.* in [PAM+10], which marked the beginning of DI randomness certification.

Formulation

Let Z be a random variable of alphabet $\mathcal{Z}$ associated to the probability distribution P_Z. Its *guessing probability* corresponds to the best prediction one could make for Z, and is thus defined as:

$$P_{\text{guess}}(Z) = \max_{z \in \mathcal{Z}} P_Z(z). \tag{2.27}$$

For a uniform distribution of alphabet size $|\mathcal{Z}| = d$, the guessing probability is $P_{\text{guess}}(Z) = 1/d$, while for a distribution containing no randomness, $P_{\text{guess}}(Z) = 1$. The *min-entropy* of Z is defined as $H_{\min}(Z) = -\log_2 P_{\text{guess}}(Z)$

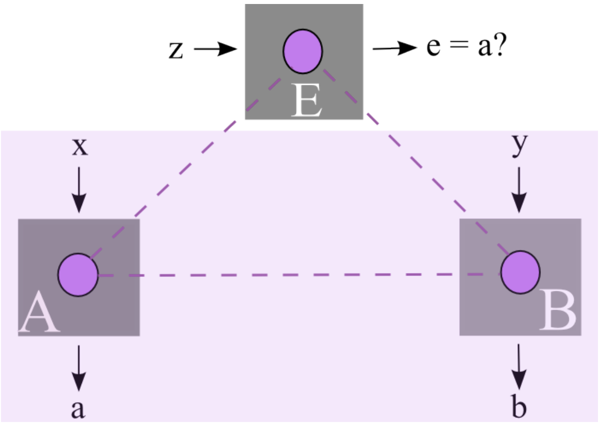

Figure 2.4.: An external observer or eavesdropper Eve is trying to guess Alice and Bob's outputs. Eve may have a system correlated to the users' devices (which are also correlated with each other). Let us say she wants to guess Alice's outcome in particular: she makes measurement z on her system, obtains outcome e, and succeeds when her guess matches Alice's outcome $e = a$. The maximal probability of Eve making the right guess is the local guessing probability.

and is measured in bits. Since the guessing probability corresponds to the best prediction, H_{min} measures the "worst", or minimal, entropy. It is equal to 0 when there is no randomness, while its maximal value for a distribution of alphabet size d is $H_{\text{min}}(Z) = \log_2 d$.

In a Bell experiment, we consider the conditional guessing probability and min-entropy of the outputs, for some given inputs x^* and y^*. More precisely, we denote the *local* guessing probability for Alice for a given input x^* as $P_{\text{guess}}^{x^*} = \max_a P(a|x^*)$, and similarly for Bob. The *global* guessing probability for Alice and Bob for given inputs x^*, y^* is denoted $P_{\text{guess}}^{x^*,y^*} = \max_{ab} P(ab|x^*y^*)$. We can see the guessing probability as a game in an adversarial setting, where an *eavesdropper* Eve is trying to make the best possible guess about Alice and Bob's distributions. To do that, Eve should choose the outcome with highest probability, which is exactly the guessing probability. Figure 2.4 represents the guessing probability game.

The guessing probability can be quantified given the violation of a Bell inequality. Let us formulate the problem for the global guessing probability (the local version ensues straightforwardly), for inputs x^* and y^*:

$$P_{\text{guess}}^{x^*,y^*} = \max_{\vec{p}} \max_{ab} \quad P(ab|x^*y^*)$$

$$\begin{aligned} \text{such that} \quad & I = \sum_{abxy} k_{abxy} P(ab|xy) = q, \\ & \vec{p} \in \mathcal{Q}, \end{aligned} \tag{2.28}$$

where q is the observed value of Bell expression I. The maximisation is done over all possible behaviours $\vec{p}$ that belong to the quantum set and that could give rise to value q of the Bell expression. This is the way the problem was first formulated in [PAM+10]. The min-entropy as a function of the Bell inequality violation is however not necessarily convex –it was suggested to simply take the convex hull when needed. Another solution is to consider all the possible convex combinations over the outputs to define the guessing probability as $\sum_{\alpha\beta} p^{\alpha\beta} P(\alpha\beta|x^*y^*)$ with $\alpha, \beta = 0, \dots, d-1$ [BSS14]. By redefining $P_{\alpha\beta}(\alpha\beta|x^*y^*) = p^{\alpha\beta} P(\alpha\beta|x^*y^*)$, one has:

$$\begin{aligned} P_{\text{guess}}^{x^*,y^*} = \quad \max\nolimits_{\vec{p}_{\alpha\beta}} \max\nolimits_{\alpha\beta} \quad & \sum_{\alpha\beta} P_{\alpha\beta}(\alpha\beta|x^*y^*) \\ \text{such that} \quad & I = \sum_{abxy} k_{abxy} P_{\alpha\beta}(ab|xy) = q, \\ & \sum_{\alpha\beta} \sum_{ab} P_{\alpha\beta}(ab|xy) = 1, \\ & \vec{p}_{\alpha\beta} \in \tilde{\mathcal{Q}}. \end{aligned} \tag{2.29}$$

The maximisation is done over vectors $\vec{p}_{\alpha\beta}$ which are now unnormalised probability distributions from the redefinition of $P_{\alpha\beta}$. The behaviour $\vec{p}_{\alpha\beta}$ must be quantum, more precisely it must belong to the unnormalised quantum set $\tilde{\mathcal{Q}}$. The resulting function of the min-entropy versus the Bell inequality violation is now convex. It turns out that this formulation also allows the certification to be based on the full behaviour instead of a Bell inequality violation only [NSPS14, BSS14], by changing one of the conditions:

$$\begin{aligned} P_{\text{guess}}^{x^*,y^*} = \quad \max\nolimits_{\vec{p}_{\alpha\beta}} \max\nolimits_{\alpha\beta} \quad & \sum_{\alpha\beta} P_{\alpha\beta}(\alpha\beta|x^*y^*) \\ \text{such that} \quad & \sum_{\alpha\beta} \vec{p}_{\alpha\beta} = \hat{\vec{p}}, \\ & \vec{p}_{\alpha\beta} \in \tilde{\mathcal{Q}}, \end{aligned} \tag{2.30}$$

where $\hat{\vec{p}}$ is the vector containing the observed frequencies $\hat{P}(ab|xy)$ from the Bell test. Using all the statistics yields at least as much randomness as considering the violation of a Bell inequality only – variations of the problem including the use of several Bell estimators were studied in [NSBSP18].

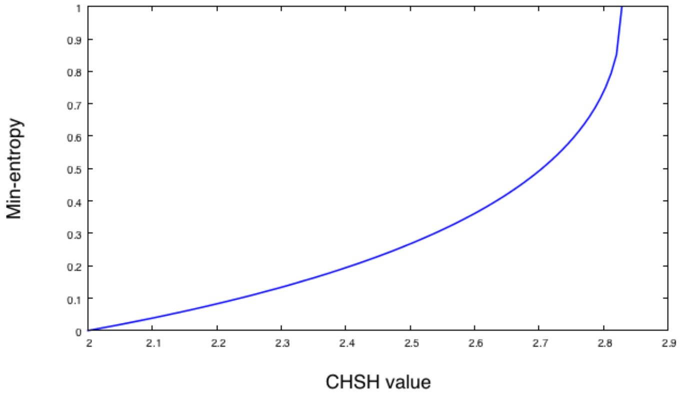

Figure 2.5.: Local min-entropy as a function of the value of the CHSH expression, obtained with the NPA hierarchy at level 2. The value $I_{CHSH} = 2$ is still compatible with an LHV model, hence no randomness is guaranteed. The min-entropy increases monotonically until the maximal quantum violation $I_{CHSH} = 2\sqrt{2}$, where 1 bit of local randomness is certified.

Problems (2.28), (2.29) and (2.30) can all be relaxed as SDPs using the NPA hierarchy, and thus solved numerically. Indeed, conditions of the type $\vec{p} \in \mathcal{Q}$ can be relaxed using the NPA sets $\mathcal{Q}_k$. Let us show an example of the local randomness certified by the CHSH inequality in Figure 2.5. Analytical bounds on the randomness can also be found, as in [PAM+10], but were obtained only in a few cases.

In this thesis, we focus on the certification of randomness as presented above – however, this certification can be made in the context of a larger DI randomness expansion protocol. The outline of such a protocol, as presented in [PM13], would be :

- **Bell experiment:** Alice and Bob perform n measurements using their devices, with inputs $(x_1, y_1) \dots (x_n, y_n)$ and outputs $(a_1, b_1) \dots (a_n, b_n)$.

- **Min-entropy evaluation:** They estimate a Bell expression $\hat{I}$, and obtain a bound on the min-entropy of their string of outputs as a function of the Bell expression value: $H_{\text{min}}^n \geq f(\hat{I}, n)$. They can also obtain this bound from the estimated behaviour $\hat{\vec{p}}$ (i.e. from the full statistics).

- **Randomness extraction:** Alice and Bob process their string of outputs into a smaller string, uniform and fully random with respect to an adversary, and the length of the resulting string depends on the min-entropy of their string of outputs H^n_{min}, estimated from the observed Bell violation.

State of the art

In the protocol we just outlined, different assumptions can be made to prove security: for instance, whether the adversary possesses classical or quantum side information. As argued in [PM13], it is reasonable to assume classical side information when considering practical situations where the manufacturer of the devices is trusted. In this case, the randomness extraction step is fully classical, but note that there exist extractors for quantum side information as well [DPVR12]. In their recent work, Arnon-Friedman *et al.* present protocols that are secure against quantum adversaries [AFDF$^+$18]. Moreover, they address the crucial i.i.d assumption that had often been used in DI protocols without the existence of a result relating the general case to the i.i.d case. In their work, they derive the so-called "entropy accumulation theorem" which characterises the amount of entropy accumulated in a sequential process where each step does not have to behave identically and independently. Then, they show how this theorem can be applied to prove full security of DI protocols in the general case (in the protocol above, to obtain bounds on the min-entropy of the whole sequence of outputs H^n_{min}).

Note that the terminology randomness *expansion* is often used because the protocol requires a small initial seed of randomness to generate the inputs to the devices, since the first step of the protocol consists in performing a Bell test. Then, a protocol is useful only if it produces more randomness than it consumes, so its efficiency is measured by the ratio between the output string and the initial seed (note that some randomness is also used in the extraction step). It is however argued in [PM13] that in a practical DI scenario where the manufacturer of the devices is considered honest, the initial seed does not need to be private with respect to the adversary and can just consist of public randomness –the terminology *private randomness generation* is then used.

When focusing on the quantification of the min-entropy without taking into account the entire protocol (as we do in this thesis), the terminology randomness *certification* is often used. This approach consists in deriving min-entropy bounds and studies the resources necessary for randomness. It answers questions such as: from which states is it possible to extract randomness and what amount of it? For instance, from the singlet state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, 1 bit of local randomness can be certified using the CHSH inequality [PAM$^+$10], and 2 bits of global randomness by adding an extra measurement to the CHSH setting, or by using the chained Bell inequalities [DPA13].

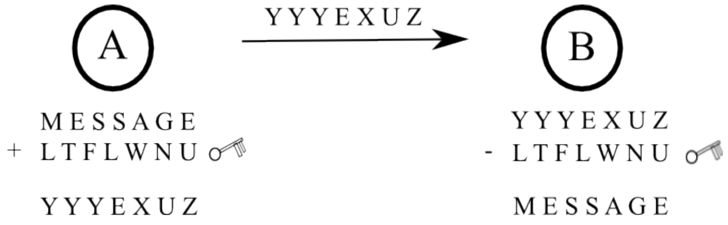

Figure 2.6.: One-time pad or Vernam cipher. Alice encodes her message using a secret key that was pre-shared with Bob. She then sends the encoded message on a public channel, which Bob decodes with the same key. The scheme is only secure if the key is used once, hence the name one-time pad.

Special scenarios have also been studied: for instance, Acín *et al.* showed that by applying POVMs, 2 bits of local randomness can be certified from the singlet [APVW16]. Curchod *et al.* proved that by using sequential measurements, any amount of local randomness can be certified from a pair of qubits in a pure state [CJA+17]. In general, the relation between randomness, nonlocality and entanglement is not straightforward: for instance, Acín, Massar and Pironio showed that 1 bit of local randomness can be certified from any partially entangled state of two qubits $|\psi_\theta\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle$, however small the angle θ may be [AMP12].

2.3.3. Quantum key distribution

Motivation

A central problem in cryptography is the distribution of secret keys among users. Distant users that possess pre-shared secret keys can use them to encrypt the messages they send to each other. A simple encryption scheme, the *one-time pad* or Vernam cipher, is explained in Figure 2.6. It turns out that quantum systems can be employed for this task.

The intuition behind quantum key distribution (QKD) comes from the following fundamental observation: Eve cannot gain any information from the qubits transmitted from Alice to Bob without disturbing their state [NC11]. QKD is a popular and relatively mature topic in quantum information theory – it was performed over long distances in several experiments [SGG+02, LYL+17]. An example of a protocol is the famous BB84 [BB84].

All this is device dependent, but it turns out that QKD can also be done in the DI framework [ABG+07, VV14, MA16]. In this section, we focus on a class of protocols studied in [MPA11], which we will be using in Chapter 4.

A class of QKD protocols

Let us give the outline of the protocol:

- **Measurements:** Alice and Bob make measurements on the copies of bipartite quantum systems that are distributed to them. For a number of rounds n, their inputs are set to fixed values, $x = x^*$ and $y = y^*$, and the outcomes they obtain constitute their two versions of the raw key $\vec{a} = (a_1, a_2, \cdots, a_n)$ and $\vec{b} = (b_1, b_2, \cdots, b_n)$. For a small number of rounds, which can be taken for instance as $n_{\text{est}} = \sqrt{n}$, the inputs are chosen uniformly at random so that they perform a proper Bell test.

- **Bell estimation:** The outputs of the n_{est} rounds are used to estimate the violation of a Bell inequality or the degree of nonlocality of their correlations in general.

- **Information reconciliation:** Alice and Bob perform error-correction to obtain identical secret keys, thus sacrificing part of their bits. This can be done by Alice publishing a message about $\vec{a}$ which is then used by Bob to correct his errors.

- **Privacy amplification:** Alice and Bob obtain a new, shorter key to reduce the knowledge of Eve about their key even further. They can do this by applying a two-universal hash function to their keys.

It is important to note that the type of the rounds in the first step is not predetermined, so that an eavesdropper Eve cannot know if a given round will be a key generation round or a Bell test round. The figure of merit for the protocol is the asymptotic *key generation rate* K, which expresses the amount of bits generated per round (in the ideal case, no finite size corrections). It can be lower bounded as follows:

$$K \geq I(A_{x^*} : B_{y^*}) - \chi(A_{x^*} : E), \tag{2.31}$$

This is the Devetak-Winter rate [DW05], where $I(A : B) = H(A) - H(A|B)$ is the mutual information between Alice and Bob, here for inputs x^* and y^*. H is the Shannon entropy, and $\chi(A : E)$ is the Holevo quantity between Alice and the eavesdropper Eve, which can be expressed as $\chi(A : E) = H(A) - H(A|E)$. Expression (2.31) thus becomes $K \geq H(A_{x^*}|E) - H(A_{x^*}|B_{y^*})$ [Ren05]. A bound on the key rate as a function of the CHSH inequality violation was found in

[PAB$^+$09]. This result is valid when restricting the eavesdropper to collective attacks (i.e. assuming i.i.d actions of Eve on Alice and Bob's systems). It was recently extended to the general case by Arnon-Friedman *et al.* [AFDF$^+$18].

Computing the conditional Shannon entropy $H(A|E)$ as a function of a Bell inequality violation is in general a difficult task, but this quantity can be lower-bounded by the min-entropy $H_{\min}(A|E)$, for which there exist numerical methods. This lower bound is not tight in general and some efficiency is likely to be lost, but the key rate becomes easier to compute:

$$K \geq H_{\min}^{x^*} - H(A_{x^*}|B_{y^*}). \tag{2.32}$$

The first term is the local min-entropy of Alice for input x^* and can be bounded as a function of the Bell inequality violation estimated in the second step, as explained in Section 2.3.2. It quantifies the amount of private randomness in the string of outcomes of Alice, i.e. it expresses how secure the secret key is with respect to an external observer. The second term is the conditional Shannon entropy between Alice and Bob, defined as $H(A_{x^*}|B_{y^*}) = \sum_{a,b} -P(ab|x^*y^*)\log_d P(a|bx^*y^*)$. It expresses the amount of bits necessary for the error correction step [CK78], and is thus related to how well Alice and Bob's outcomes are correlated.

The key rate can be studied as a function of the visibility or the amount of noise present in the quantum state used for the protocol. The *critical visibility* is the value at which the key generation rate reaches 0: for instance it is close to ~ 0.9 for the CHSH inequality [MPA11]. This makes the protocol comparable to standard QKD in terms of noise robustness.

2.3.4. Self-testing

Motivation

Instead of using nonlocality to certify a quantity or property such as randomness, it is also possible to use the correlations produced by the black boxes of a Bell test to certify what was exactly inside those black boxes: this is the aim of *self-testing*. Self-testing was introduced by Mayers and Yao in [MY04], and has received a lot of attention in the last few years.

Imagine a user who receives a "black box apparatus" that displays nonlocal correlations from a provider. The provider claims that these boxes perform some specific measurements on a given quantum state, and the user would like to verify this claim and make sure the boxes work properly. This is particularly relevant if the user does not trust the provider or does not want to rely on the provider's ability to prepare the devices, or simply wants to verify that the apparatus keeps functioning correctly over time. Self-testing is the DI protocol the user has to follow to complete this goal. The self-tested states and measurements can then be used for another quantum information protocol – Mayers and Yao [MY04] suggested it for quantum key distribution.

Self-testing is also a goal in itself. On the foundational level, self-testing gives us insight into the structure of the quantum set. Indeed, a nonlocal behaviour $\vec{p}$ needs to demonstrate some form of "uniqueness" to be self-tested: the correlations must point to a unique state and measurements (up to some degrees of freedom as we will see below), otherwise they could also be explained by a set of state and measurements which are not the ones that are supposed to be self-tested. In particular, when considering a specific Bell inequality, its maximal quantum violation should be unique for the Bell inequality to be useful for self-testing. This is often the case, but not always (see [GKW$^+$18]).

Definitions

Let us introduce the self-testing terminology. The *reference experiment* is the specification of the black boxes (in our example, the claim made by the provider). It consists of the reference state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and reference measurements $M_{a|x}, N_{b|y}$. On the other hand, what is really happening inside the black boxes is called the *physical experiment*. The physical state and measurements are denoted $\{|\psi'\rangle, M'_{a|x}, N'_{b|y}\}$, with $|\psi'\rangle$ in a product Hilbert space of unrestricted dimension $\mathcal{H}'_A \otimes \mathcal{H}'_B$.

The goal is to compare the reference and the physical experiment and certify that they are physically equivalent. This notion of equivalence must allow for local changes of basis, and also for additional degrees of freedom to be present in the boxes. Mathematically, we require:

$$\begin{aligned} |\psi'\rangle &= U_{AA'} \otimes U_{BB'} |\psi\rangle_{AB} |\varphi\rangle_{A'B'} \\ M'_{a|x} \otimes N'_{b|y} |\psi'\rangle &= U_{AA'} \otimes U_{BB'} \left(M_{a|x} \otimes N_{b|y} |\psi\rangle_{AB} \right) |\varphi\rangle_{A'B'}, \end{aligned} \tag{2.33}$$

where $U_{AA'}$ and $U_{BB'}$ are arbitrary local unitaries and $|\varphi\rangle_{A'B'}$ describe the local states of the possible additional degrees of freedom of the physical experiment. Here $|\varphi\rangle_{A'B'}$ is often referred to as the *junk state*. The idea behind this "junk state" is the following: it is not possible to have a single isolated qubit in practice – if you measure the spin of the electron, the whole electron with its wave function is also there. The physical state in the black boxes can thus contain extra degrees of freedom, but those should be in tensor product with the reference state.

The notion of equivalence we just described is contained in the concept of local isometry, a map that preserves the inner product but does not have to preserve dimension, in our case a product isometry $\Phi = \Phi_A \otimes \Phi_B : \mathcal{H}'_A \otimes \mathcal{H}'_B \to \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}'_A \otimes \mathcal{H}'_B$. Thus, a self-testing protocol is successful if there exists a local isometry relating the physical and reference experiments:

$$\begin{aligned} \Phi\left(|\psi'\rangle\right) &= |\psi\rangle|\varphi\rangle \\ \Phi\left(M'_{a|x} \otimes N'_{b|y}|\psi'\rangle\right) &= \left(M_{a|x} \otimes N_{b|y}|\psi\rangle\right)|\varphi\rangle. \end{aligned} \tag{2.34}$$

The existence of this isometry can be proven from the full statistics of a Bell test, or from the maximal violation of a Bell inequality. The physical and reference experiments must then yield the same vector of correlations $\vec{p}$, or the same maximal violation of a Bell inequality, which is a weaker necessary condition.

In practice however, one does not expect to observe the exact maximal violation of a Bell inequality, or an exact behaviour. It turns out that self-testing statements can still be formulated even if the observed correlations contain some noise. For instance, if the observed value of the Bell expression is ϵ-close to the maximal violation β_Q, robust self-testing statements should be of the form:

$$\begin{aligned} ||\Phi\left(|\psi'\rangle\right) - |\psi\rangle|\varphi\rangle|| &\leq f(\epsilon) \\ ||\Phi\left(M'_{a|x} \otimes N'_{b|y}|\psi'\rangle\right) - \left(M_{a|x} \otimes N_{b|y}|\psi\rangle\right)|\varphi\rangle|| &\leq f'(\epsilon), \end{aligned} \tag{2.35}$$

where f and f' are functions of ϵ that vanish as $\epsilon \to 0$.

Finally, note that we took the states to be pure and the measurements projective, as it is more convenient to work with those, and it is what is done in most self-testing publications. This is possible because the dimension of the Hilbert space in the black boxes is not constrained. To be more precise, if the physical state $\rho_{A'B'}$ is not pure, then a purification $|\psi'\rangle_{A'B'P}$ can be taken where $\mathcal{H}_P$ is the purification space. The isometry should then be such that $\Phi \otimes \mathbb{I}_P$, with only the identity channel acting on the purification space.

An example: self-test based on the CHSH inequality

We present an example which will both clarify the above definitions and illustrate one of the methods to prove self-testing to the reader. This is the self-test of the singlet based on the maximal violation of the CHSH inequality. The reference experiment is the following:

$$\begin{aligned} |\psi\rangle = |\phi^+\rangle &= \tfrac{|00\rangle+|11\rangle}{\sqrt{2}} \\ A_1 = X, &\quad A_2 = Z, \\ B_1 = \tfrac{X+Z}{\sqrt{2}}, &\quad B_2 = \tfrac{X-Z}{\sqrt{2}}, \end{aligned} \tag{2.36}$$

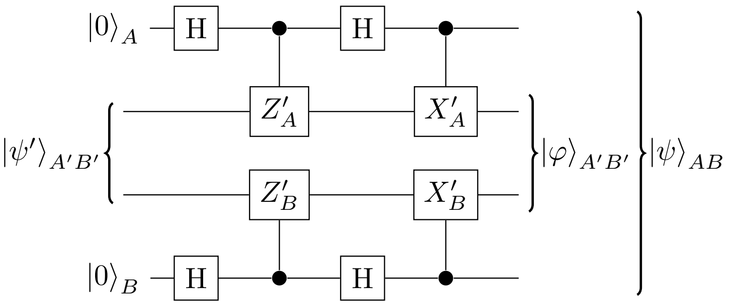

Figure 2.7.: Swap gate isometry for self-testing. The Z'_A and Z'_B operations are functions of the physical measurements, and should act like controlled-Z gates on the physical state. Similarly, the X'_A and X'_B should act like controlled-X gates. H is the standard one-qubit Hadamard gate. At the end of the circuit, the reference state is found in tensor product with the junk state.

where X and Z refer to the Pauli matrices, and the A_i and B_i are measurement observables (the clearest notation for the CHSH case).

Figure 2.7 represents the self-testing isometry as a circuit. The circuit acts as a swap gate between controlled ancillary systems and the state $|\psi'\rangle$ in the black boxes: at the end of the circuit, the reference state has been "extracted" to the ancillas and what is left in the boxes is the junk state $|\varphi\rangle_{A'B'}$. For the swap to function, the gates in the circuit should act, respectively, as controlled-Z and controlled-X gates on the physical state. This should happen perfectly in the ideal case: hence, we can use the reference measurements as an intuition to define the gates in terms of the physical measurements. We choose: $Z'_A = A'_2$, $X'_A = A'_1$, $Z'_B = (B'_1 - B'_2)/\sqrt{2}$ and $X'_B = (B'_1 + B'_2)/\sqrt{2}$. One can verify that the state after the action of the isometry is:

$$\begin{aligned}\Phi\left(|\psi'\rangle\right) =& \frac{1}{4}\big[(\mathbb{I}+Z'_A)(\mathbb{I}+Z'_B)|\psi'\rangle_{A'B'}\otimes|00\rangle_{AB}\\ &+X'_B(\mathbb{I}+Z'_A)(\mathbb{I}-Z'_B)|\psi'\rangle_{A'B'}\otimes|01\rangle_{AB}\\ &+X'_A(\mathbb{I}-Z'_A)(\mathbb{I}+Z'_B)|\psi'\rangle_{A'B'}\otimes|10\rangle_{AB}\\ &+X'_AX'_B(\mathbb{I}-Z'_A)(\mathbb{I}-Z'_B)|\psi'\rangle_{A'B'}\otimes|11\rangle_{AB}\big].\end{aligned} \tag{2.37}$$

We must show the right hand side of (2.37) is equal to the reference state in tensor product with a junk state$|\psi\rangle|\varphi\rangle$. To this end we will use SOS decompositions (see equation (2.20)) of the shifted CHSH Bell operator $\tilde{\mathcal{B}}_{CHSH} =$

$2\sqrt{2}\mathbb{I} - \mathcal{B}_{CHSH}$. A decomposition of the first order can be written as:

$$\tilde{\mathcal{B}}_{CHSH} = \frac{1}{\sqrt{2}}\left[\left(A_1 - \frac{B_1+B_2}{\sqrt{2}}\right)^2 + \left(A_2 - \frac{B_1-B_2}{\sqrt{2}}\right)^2\right], \tag{2.38}$$

where P_λ^2 is used istead of $P_\lambda^\dagger P_\lambda$ since all the operators are hermitian. A second order decomposition can be found:

$$\tilde{\mathcal{B}}_{CHSH} = \frac{1}{4\sqrt{2}}\left[\mathcal{B}^2_{CHSH} + 2\left(A_2\frac{B_1+B_2}{\sqrt{2}} + A_1\frac{B_1-B_2}{\sqrt{2}}\right)^2\right]. \tag{2.39}$$

When the maximal violation $2\sqrt{2}$ is observed, we have that $\langle\psi'|\tilde{\mathcal{B}}_{CHSH}|\psi'\rangle = 0$. Hence, each term of the SOS decomposition acting on the physical state must be equal to 0 as well. More precisely, $\langle\psi'|P_\lambda^\dagger P_\lambda|\psi'\rangle = 0$, which implies $P_\lambda|\psi'\rangle = 0$. These relations can be used to prove that the isometry does indeed send the physical state to the reference state in tensor product with a junk state. This is a method that can be used for other any Bell operator, as long as appropriate SOS decompositions can be found. From the decompositions (2.38) and (2.39), the following relations can be found:

$$\begin{aligned}
&(Z'_A - Z'_B)|\psi'\rangle = 0\\
&(X'_A - X'_B)|\psi'\rangle = 0\\
&(X'_A Z'_A + Z'_A X'_A)|\psi'\rangle = 0\\
&(X'_B Z'_B + Z'_B X'_B)|\psi'\rangle = 0.
\end{aligned} \tag{2.40}$$

One can apply these relations to expression (2.37) and verify that they are sufficient to prove that $\Phi\left(|\psi'\rangle\right) = |\psi\rangle|\varphi\rangle$. This concludes the self-test of the singlet state $|\psi\rangle = |\phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. The self-test of the measurements can be done in a similar fashion.

The SWAP method

It is not always easy to solve a self-testing problem analytically as in the CHSH case. However, there exists a numerical approach called the SWAP method which was proposed in [YVB+14, BNS+15] and which is based on the NPA hierarchy. In particular, it allows one to lower bound the fidelity between the reference and physical states given the violation of a Bell inequality. In more precise terms, it solves an SDP which typically has the form:

$$\begin{aligned}
F = \quad \min \quad & \langle\psi|\rho_{\text{swap}}|\psi\rangle\\
\text{s.t.} \quad & c \in \mathcal{Q}_k\\
& I = q.
\end{aligned} \tag{2.41}$$

where ρ_{swap} is the physical state on which the swap operation $\mathcal{S}$ was applied, and $|\psi\rangle$ is the reference state. This swapped state is defined as:

$$\rho_{\text{swap}} = \text{tr}_{A'B'} \left[\mathcal{S} \rho'_{A'B'} \otimes |00\rangle\langle 00|_{AB} \mathcal{S}^{\dagger} \right] \tag{2.42}$$

with $\rho'_{A'B'} = |\psi'\rangle\langle\psi'|$, and $|00\rangle\langle 00|_{AB}$ are ancillary states. The swap operation $\mathcal{S} = \mathcal{S}_{AA'} \otimes \mathcal{S}_{BB'}$ is composed of local unitaries $\mathcal{S}_{AA'}$ and $\mathcal{S}_{BB'}$, so that the operation $\mathcal{S}$ together with the introduction of the ancillary states constitute the local isometry defining the self-test as in expression (2.34).

The idea is that $\mathcal{S}$ should be written in terms of the physical measurements $M'_{a|x}, N'_{b|y}$ (proceeding, for instance as in Figure 2.7 and the CHSH example provided). One can verify that the objective function F can then be written as a sum of elements of an NPA moment matrix – for the corresponding scenario and appropriate level of the hierarchy. This is expressed by the condition $c \in \mathcal{Q}_k$. The letter q denotes the observed value of the Bell expression I. When the maximal violation is observed, i.e. $q = \beta_Q$, we expect to obtain a minimum fidelity $F = 1$ (up to numerical precision) in order to conclude that the self-test is successful. Note that it can happen that $\mathcal{S}$ is not a properly defined isometry as it may contain some non-unitary operations: this can be fixed but introduces extra conditions in problem (2.41) of the form $\Gamma_A \succeq 0, \Gamma_B \succeq 0$ where Γ_A and Γ_B are so-called localising matrices.

To sum up, solving problem (2.41) amounts to finding the quantum state that minimises its fidelity to the reference state while remaining compatible with the experimentally observed correlations. Self-testing requires an almost ideal experimental setting, as by being far from the maximal quantum violation of a Bell inequality one will rapidly find orthogonal states yielding the same observed statistics, thus rendering self-testing impossible. The SWAP method provides however stronger bounds than most of the analytical methods.

State of the art

Mayers and Yao described in [MY04] a procedure to self-test the singlet state, which was made robust by McKague *et al.* in [MYS12]. The SWAP method gave better robustness bounds on this self-test, and also allowed for the self-test of the partially entangled state of two qutrits $|\psi_\gamma\rangle = (|00\rangle + |11\rangle + |22\rangle)/(\sqrt{2+\gamma^2})$, with $\gamma = (\sqrt{11} - \sqrt{3})/2$, which is the state maximally violating the CGLMP Bell inequality for 3 outcomes [CGL$^+$02, ADGL02]. All partially entangled two-qubit states were self-tested in [BP15] using the tilted CHSH inequalities [AMP12]. Finally, it was shown by Coladangelo *et al.* [CGS17] that all pure bipartite entangled states (of any dimension) can be self-tested.

The multipartite case remains to be studied –an approach to self-test multipartite states by projection onto two systems was presented in [ŠCAA18]. Self-testing of graph states was achieved by McKague in [McK14]. The SWAP method was also used for the self-test of some multipartite states, such as the GHZ and W states [PVN14, WCY$^+$14].

Self-testing scenarios that depart from the definitions given in this chapter have also been studied. Kaniewski introduced in [Kan16] a new technique to obtain self-testing bounds analytically which greatly improved the robustness for the singlet and GHZ states. He also considered the question of measurement self-testing, which is considerably less studied than state self-testing, in [Kan17]. Bowles *et al.* used self-testing to construct a protocol that certifies the entanglement of all bipartite entangled quantum states in a DI way [BŠCA18a, BŠCA18b].

2.3.5. Experimental device-independent protocols

The implementation of DI quantum information protocols is not as mature as its device dependent counterpart. On the one hand, there are the loopholes mentioned in Section 2.2.5. On the other hand, the presence of noise can quickly affect the success of DI protocols: if the observed violation of the Bell inequality is not high enough, the amount of randomness may be very small, or the key generation rate null, depending on the robustness of the protocol. Reference [MA16] contains a recent analysis of implementations for DIQKD, and proposals to overcome those challenges. DI randomness certification was first performed as a proof-of-concept in the initial paper of Pironio *et al.* [PAM$^+$10]. Several experiments followed: detection-loophole-free in [CMA$^+$13], loophole-free in [BKG$^+$18], and using non-projective measurements in [GMG$^+$18]. Reference [AM16] reviews approaches as well as implementations for DI randomness certification.

3. Chained Bell inequalities: self-testing and randomness certification

In this chapter we study how the chained Bell inequalities can be used to build self-testing protocols. We mentioned in Chapter 2 that many of the known self-tests are constructed from the maximal violation of a Bell inequality. Based on geometrical considerations [FFW11, DPA13], one expects that there is a unique way of producing the extremal correlations attaining the maximal quantum violation of a Bell inequality, i.e. a unique state and measurements. This is not always the case [GKW$^+$18], but whenever it is, we say that the corresponding Bell inequality is *useful for self-testing*. 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.

The chained Bell inequalities were introduced in [Pea70, BC90] for a bipartite Bell scenario with an arbitrary number of measurements of two outputs each. Their maximal quantum violation is given by the maximally entangled state of two qubits, and measurements equally spaced on an equator of the Bloch sphere [Weh06]. The singlet state has been self-tested through various schemes [MY04, MYS12, MS13] – so, with our self-test, we provide an additional method. The advantage of our approach over the previous results lies in the self-testing of the measurements: in the limit of a large number of measurements, the chained Bell inequalities allows us to self-test the entire plane of the Bloch sphere spanned by the Pauli matrices X and Z. Our self-test also shows that the maximal violation of the chained Bell inequalities is unique. This makes them useful for randomness certification, following the results of [DPA13].

We start by introducing the chained Bell inequalities and we find SOS decompositions which allow us to prove self-testing for any number m of inputs. We then study the robustness of the protocol, and show that randomness certification can be performed.

3.1. The chained Bell inequalities

The chained Bell inequalities were introduced in [Pea70, BC90] to generalise the well-known CHSH Bell inequality [CHSH69] to a larger number of measurements per party, while keeping the number of outcomes to two. Keeping the usual CHSH notation, let us denote by A_i and B_i ($i = 1, \ldots, m$) the measurement observables of Alice and Bob, respectively, and assume that they all have outcomes ±1. Then, the chained Bell inequality for m inputs reads

$$I_{\text{ch}}^{m} = \sum_{i=1}^{m} (\langle A_i B_i \rangle + \langle A_{i+1} B_i \rangle) \leq 2m - 2, \tag{3.1}$$

where we denote $A_{m+1} \equiv -A_1$. Notice that for $m = 2$ the above formula reproduces the CHSH Bell inequality

$$\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_2 B_2 \rangle - \langle A_1 B_2 \rangle \leq 2. \tag{3.2}$$

Importantly, in quantum theory the chained Bell inequality can be violated by Alice and Bob if they perform measurements on an entangled quantum state. The associated Bell operator is

$$\mathcal{B}_m = \sum_{i=1}^{m} \left(A_i \otimes B_i + A_{i+1} \otimes B_i \right), \tag{3.3}$$

where again $A_{m+1} \equiv -A_1$. It was shown by Wehner [Weh06] that the Bell operator is upper bounded by

$$B_m^{\max} = 2m \cos \frac{\pi}{2m}. \tag{3.4}$$

There exists a quantum realisation attaining this bound, hence $B_m^{\max}$ is the tight Tsirelson bound of the chained Bell inequality (3.1) $\beta_Q = B_m^{\max}$. This realisation is the following: the state is the maximally entangled state of two qubits, or singlet,

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{3.5}$$

and the measurements are

$$A_i = s_i X + c_i Z, \qquad B_i = s_i' X + c_i' Z, \tag{3.6}$$

where X and Z are the standard Pauli matrices and $s_i = \sin \phi_i$, $c_i = \cos \phi_i$, $s_i' = \sin \phi_i'$ and $c_i' = \cos \phi_i'$, where $\phi_i = [(i-1)\pi]/m$ and $\phi_i' = [(2i-1)\pi]/2m$. These are thus our reference state and measurements for the self-test, and the measurements are represented in Figure 3.1.

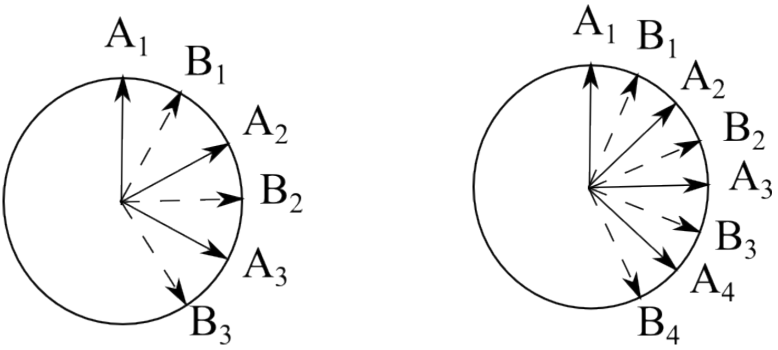

Figure 3.1.: Representation of the optimal measurements A_i and B_i on the XZ plane of the Bloch sphere with $i = 1, \dots, m$. The case of three measurement choices ($m = 3$) is on the left, and the case of four measurement choices ($m = 4$) is on the right. As m grows, the distribution of measurements remains similar: A_1 is always Z, and X is given by $A_{m/2+1}$ for even m and by $B_{(m+1)/2}$ for odd m.

3.2. Sum-of-squares decompositions

We introduce SOS decompositions (see (2.20)) of the first and second order for the shifted Bell operator $\tilde{\mathcal{B}}_m = B_m^{\max}\mathbb{I} - \mathcal{B}_m$. As seen in the CHSH example of Section 2.3.4, these decompositions yield conditions on the state and measurements maximally violating the Bell inequality which will allow us to prove self-testing.

3.2.1. First order decompositions

Lemma 3.1. *Let $\{|\psi'\rangle, A_i', B_i'\}$ be the state and the measurements maximally violating the chained Bell inequality. Then, the corresponding shifted Bell operator $\tilde{\mathcal{B}}_m = B_m^{\max}\mathbb{I} - \mathcal{B}_m$ admits the following first-order SOS decomposition:*

$$B_m^{\max}\mathbb{I} - \mathcal{B}_m = \cos\frac{\pi}{2m}\left[\sum_{i=1}^{m}\left(\mathbb{I} - A_i' \otimes \frac{B_i' + B_{i-1}'}{2\cos(\pi/2m)}\right)^2 + \frac{1}{m}\sum_{j=1}^{m}\sum_{i=1}^{m-2}\left(\alpha_i B_j' + \beta_i B_{i+j}' + \gamma_i B_{i+j+1}'\right)^2\right], \tag{3.7}$$

where we assume that $B'_{m+j} = -B'_j$ *and* $B'_m = -B'_0$*. The coefficients* α_i*,* β_i*, and* γ_i *are given by*

$$\alpha_i = \frac{\sin(\pi/m)}{2\cos(\pi/2m)}\sqrt{\frac{1}{\sin(\pi i/m)\sin[\pi(i+1)/m]}}, \tag{3.8}$$

$$\beta_i = \frac{-1}{2\cos(\pi/2m)}\sqrt{\frac{\sin[\pi(i+1)/m]}{\sin(\pi i/m)}}, \tag{3.9}$$

and

$$\gamma_i = \frac{1}{2\cos(\pi/2m)}\sqrt{\frac{\sin(\pi i/m)}{\sin[\pi(i+1)/m]}} = -\frac{1}{4\beta_i\cos^2(\pi/2m)} \tag{3.10}$$

with $i = 1, \ldots, m-2$*.*

Let us clarify how the validity of SOS decomposition (3.7) can be verified. First, one expands the first sum of the right-hand side and notices that apart from the terms forming the shifted Bell operator $B_m^{\max}\mathbb{I} - \mathcal{B}_m$ there are some additional terms of the form $B'_k B'_{k+1}$. These are cancelled out by the same terms appearing in the second sum on the right-hand side of equation (3.7). The only trouble one has to face in reducing all the remaining terms to the shifted Bell operator is to prove that the coefficient multiplying the identity operator $\mathbb{I}$ is exactly $2m\cos(\pi/2m)$. Let us now prove that this is indeed the case. To this end, we write this coefficient as

$$\Delta = \cos\frac{\pi}{2m}\left[m + \frac{m}{2\cos^2(\pi/2m)} + \Delta_\alpha + \Delta_\beta + \Delta_\gamma\right], \tag{3.11}$$

where

$$\Delta_\omega = \sum_{i=1}^{m-2}\omega_i^2 \tag{3.12}$$

with $\omega = \alpha, \beta, \gamma$. Recall that the coefficients α_i, β_i and γ_i are defined in equations (3.8), (3.9) and (3.10). Let us now compute each term Δ_ω separately, starting from Δ_α. Exploiting equation (3.8) we can write

$$\begin{aligned}\Delta_\alpha &= \tfrac{1}{4\cos^2(\pi/2m)}\textstyle\sum_{i=1}^{m-2}\left[\tfrac{\sin^2(\pi/m)}{\sin(i\pi/m)\sin[(i+1)\pi/m]}\right]\\ &= \tfrac{\sin(\pi/m)}{4\cos^2(\pi/2m)}\textstyle\sum_{i=1}^{m-2}\left[\tfrac{\cos(i\pi/m)}{\sin(i\pi/m)} - \tfrac{\cos[(i+1)\pi/m]}{\sin[(i+1)\pi/m]}\right]\\ &= \tfrac{\sin(\pi/m)}{4\cos^2(\pi/2m)}\textstyle\sum_{i=1}^{m-2}\left[\cot\left(\tfrac{i\pi}{m}\right) - \cot\left[\tfrac{(i+1)\pi}{m}\right]\right].\end{aligned} \tag{3.13}$$

Now, we use the fact that

$$\sum_{i=1}^{m-1} \cot\left(\frac{\pi i}{m}\right) = 0, \tag{3.14}$$

which implies that

$$\sum_{i=1}^{m-2} \cot(\frac{i\pi}{m}) = \cot(\frac{\pi}{m}), \qquad \sum_{i=1}^{m-2} \cot(\frac{(i+1)\pi}{m}) = -\cot(\frac{\pi}{m}). \tag{3.15}$$

Substituting expression (3.15) into expression (3.13) one finds that

$$\Delta_\alpha = \frac{\cos(\pi/m)}{2\cos^2(\pi/2m)}. \tag{3.16}$$

Let us then compute Δ_β. Using equation (3.9), it can be explicitly written as

$$\Delta_\beta = \frac{1}{4\cos^2(\pi/2m)}\left[\sum_{i=1}^{m-2} \frac{\sin[(i+1)\pi/m]}{\sin(i\pi/m)}\right], \tag{3.17}$$

which with the aid of the elementary trigonometric property that $\sin(x+y) = \sin x \cos y + \cos x \sin y$, rewrites as

$$\Delta_\beta = \frac{1}{4\cos^2(\pi/2m)}\left[(m-2)\cos(\frac{\pi}{m}) + \sin(\frac{\pi}{m})\sum_{i=1}^{m-2}\cot(\frac{i\pi}{m})\right]. \tag{3.18}$$

This, by virtue of (3.15), gives

$$\Delta_\beta = \frac{(m-1)\cos(\pi/m)}{4\cos^2(\pi/2m)}. \tag{3.19}$$

Let us finally compute Δ_γ. From (3.10) it can be written explicitly as

$$\Delta_\gamma = \frac{1}{4\cos^2(\pi/2m)}\left[\sum_{i=1}^{m-2} \frac{\sin(i\pi/m)}{\sin[(i+1)\pi/m]}\right]. \tag{3.20}$$

Writing then $\sin(i\pi/m) = sin[(i+1-1)\pi/m]$ and using again the above trigonometric identity, one obtains

$$\Delta_\gamma = \frac{1}{4\cos^2(\pi/2m)}\left\{(m-2)\cos(\frac{\pi}{m}) - \sin(\frac{\pi}{m})\sum_{i=1}^{m-2}\cot\left[\frac{(i+1)\pi}{m}\right]\right\}, \tag{3.21}$$

which, taking into account equation (3.15), simplifies to

$$\Delta_\gamma = \frac{(m-1)\cos(\pi/m)}{4\cos^2(\pi/2m)}. \tag{3.22}$$

Plugging expressions (3.16), (3.19) and (3.22) into (3.11) and using some elementary properties of the trigonometric functions, one eventually obtains $\Delta = 2m\cos(\pi/2m)$, as announced.

Note that the SOS decomposition (3.7) remains valid if in its second line we omit the sum over j and fix j to be any number from $\{1,\ldots,m\}$. 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 a whole family of $2m$ SOS decompositions. Let us finally mention that the above decomposition is a particular case of an SOS decomposition for a more general Bell inequality which will be presented in Chapter 4 together with an analytical method used to derive it. It turns out, however, that none of these SOS decompositions is enough for self-testing. In fact, we need an SOS decomposition of order 2, which we present below.

3.2.2. Second order decompositions

Lemma 3.2. *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 $\tilde{\mathcal{B}}_m = B_m^{\max}\mathbb{I} - \mathcal{B}_m$ admits the following second-order SOS decomposition:*

$$\begin{aligned} &B_m^{\max}\mathbb{I} - \mathcal{B}_m \\ &= \frac{1}{8m\cos\frac{\pi}{2m}}\Bigg\{2(B_m^{\max}\mathbb{I}-\mathcal{B}_m)^2 + \sum_{\substack{i,j=1\\ j\neq i,i-1}}^{m}\left[A'_i\otimes(B'_i+B'_{i-1}) - (A'_j+A'_{j+1})\otimes B'_j\right]^2 \\ &\qquad\qquad + \sum_{i=1}^{m}\left[\left(A'_i\otimes B'_i - A'_{i+1}\otimes B'_{i+1}\right)^2 + \left(A'_i\otimes B'_{i-1} - A'_{i+1}\otimes B'_i\right)^2\right]\Bigg\} \\ &+ \frac{1}{2}\cos\left(\frac{\pi}{2m}\right)\sum_{i=1}^{m-2}\left[\left(\alpha_i B'_1 + \beta_i B'_{i+1} + \gamma_i B'_{i+2}\right)^2 + \left(\alpha_i A'_1 + \beta_i A'_{i+1} + \gamma_i A'_{i+2}\right)^2\right], \end{aligned} \tag{3.23}$$

where we used the notation $A'_{m+1} = -A'_1$ and $A'_0 = -A'_m$, and the same for Bob's operators, and the α_i, β_i and γ_i are given in equations (3.8) – (3.10).

To verify the validity of the SOS decomposition (3.23) we follow a similar argumentation as for the first order SOS. The first parenthesis on the right hand side of (3.23) introduces terms that up to some multiplicative factors belong to the following set $\{\mathbb{I}, A'_iB'_i, A'_iB'_{i-1}, A'_iA'_{i+1}, B'_iB'_{i+1}, A'_iA'_jB'_kB'_l\}$. The terms $A'_iA'_jB'_kB'_l$ are directly cancelled out by the same terms stemming from the second and the third parenthesis. Then, the terms $A'_iA'_{i+1}$ and $B'_iB'_{i+1}$ enter with the coefficient $2/[8m\cos(\pi/2m)]$ and, together with the same terms resulting from the second parenthesis and entering with the coefficient $(m-2)/[8m\cos(\pi/2m)]$, they are cancelled out by those resulting from the third line of (3.23). The terms $A'_iB'_i$ and $A'_iB'_{i-1}$ give rise to the shifted Bell operator, and, finally, the identity operator $\mathbb{I}$ is multiplied by the following expression

$$\frac{1}{8m\cos(\pi/2m)}\left\{\left[8m^2\cos^2(\frac{\pi}{2m})+4m\right]+4m(m-2)+4m\right\}+\frac{m\cos(\pi/m)}{2\cos^2(\pi/2m)} \tag{3.24}$$

which after simplifications becomes $2m\cos(\pi/2m)$. This is exactly the multiplicative factor of the identity operator in the shifted Bell operator.

As for the first order SOS, we can construct another SOS decomposition from (3.23) 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.

3.3. Self-test: the ideal case

We consider the ideal case, i.e. when the black boxes reach the maximal quantum violation of the Bell inequality, and leave the study of the robustness of our protocol for the following section.

3.3.1. Outline

Let us start with a summary of our self-testing procedure. The calculations in the remainder of this chapter are rather heavy, but they are complete and self-contained – we thus invite the reader to either follow them line by line or to settle for this outline, which focuses on the intuition and refers the reader to the most important results.

- **Isometry:** First, we write down the self-testing isometry. To this end, we choose the swap circuit often used in self-testing. In this circuit, some of the gates should be functions of the measurements of Alice and Bob, and should act as controlled-Z and controlled-X in the ideal case. To determine these gates, we look for combinations of the reference measurements that correspond to the Pauli matrices X and Z. Then, we let the gates be functions the physical measurements. This way, we know that in the ideal case when the reference and physical measurements match, the circuit will perform a proper swap operation.

- **Relations from the SOS decompositions:** Then, we derive a series of lemmas that give statements about the physical measurements acting on the physical state, based only on the fact that the maximal violation of the chained Bell inequalities is observed. This is possible to do through SOS decompositions (we refer the reader to the CHSH example of Section 2.3.4). In fact, we know the kind of relations that we need to prove self-testing, as we know the output of the isometry, and we look for such relations. For example, we must prove that the X and Z gates anticommute when acting on the physical state. It is with these necessary relations in mind that we derived our second-order SOS decompositions. Thus, the reference experiment is our inspiration.

- **Self-testing theorem**: Finally, in Theorem 3.6, we apply all the lemmas in order to relate the output of the isometry to the reference state and measurements. This concludes the self-test.

The outline of Section 3.4 on robust self-testing is very similar. The spirit is the same, but the calculations are rendered more complicated by the assumption that the maximal violation is not perfectly attained.

3.3.2. The isometry

Our isometry is presented in Figure 3.2 – it is the swap gate introduced in Figure 2.7 of Section 2.3.4, with some modifications. We need gates that act like controlled-Z and controlled-X on the physical state. To this end we choose:

$$X'_A = \begin{cases} A'_{m/2+1}, & m \text{ even} \\ \dfrac{A'_{(m+1)/2} + A'_{(m+3)/2}}{2\cos(\pi/2m)}, & m \text{ odd} \end{cases}, \qquad Z'_A = A'_1 \tag{3.25}$$

and

$$X'_B = \begin{cases} \dfrac{B'_{m/2} + B'_{m/2+1}}{2\cos(\pi/2m)}, & m \text{ even} \\ B'_{(m+1)/2}, & m \text{ odd} \end{cases}, \qquad Z'_B = \frac{B'_1 - B'_m}{2\cos(\pi/2m)}. \tag{3.26}$$

Clearly, as all observables A'_i and B'_i are Hermitian and have eigenvalues ±1, Z'_A and X'_A for even m and X'_B for odd m are unitary. However, the operators X'_A

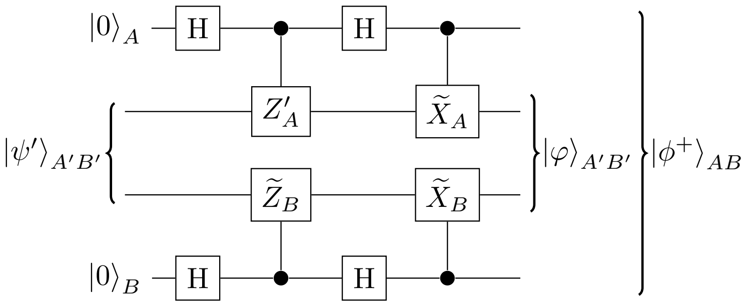

Figure 3.2.: The self-testing isometry, which is the swap gate adapted to our case. Since all the gates must be unitary, $\widetilde{X}_A$, $\widetilde{X}_B$ and $\widetilde{Z}_B$ are regularised (when needed) versions of X'_A, X'_B and Z'_B respectively. At the output of the circuit the ancillary qubits are in the desired reference state $|\phi^+\rangle$. We denote this isometry Φ, more precisely we denote by Φ the unitary operation on all the qubits $\Phi(|\psi'\rangle|00\rangle)$.

for odd m, X'_B for even m and Z'_B might not be unitary in general, which would in turn make the swap gate circuit non-unitary. To overcome this problem we exploit the polar decomposition which says that one can write any operator M as $M = U|M| = |M|V$ where U and V are some unitary operators and $|M| = \sqrt{M^\dagger M}$. Then, if say Z'_B is of full rank we define $\widetilde{Z}_B = Z'_B/|Z'_B|$, while if it is rank deficient, we replace its zero eigenvalues by one and then use the above construction; in other words, we define $\widetilde{Z}_B = (Z'_B + P)/|Z'_B + P|$ with P denoting the projector onto the kernel of Z'_B. We proceed similarly for X'_B and X'_A when needed, thus defining $\widetilde{X}_B$ and $\widetilde{X}_A$.

3.3.3. Relations from the sum-of-squares decompositions

In this section, we derive important relations from the SOS decompositions (3.7) and (3.23), which will be necessary to prove self-testing. First, we show in Lemma 3.3 that for any $i = 1, \ldots, m$, the identities

$$A'_i \otimes \frac{B'_i + B'_{i-1}}{2\cos(\pi/2m)}|\psi'\rangle = |\psi'\rangle, \qquad \frac{A'_i + A'_{i+1}}{2\cos(\pi/2m)} \otimes B_i|\psi'\rangle = |\psi'\rangle \tag{3.27}$$

are satisfied, which imply in particular that

$$X'_A|\psi'\rangle = X'_B|\psi'\rangle, \qquad Z'_A|\psi'\rangle = Z'_B|\psi'\rangle. \tag{3.28}$$

Then, we prove in Lemma 3.4 that the operators X'_A and Z'_A anticommute when acting on the physical state:

$$\{X'_A, Z'_A\}|\psi'\rangle = 0. \tag{3.29}$$

Finally, we prove relations that are necessary for the self-testing of the measurements in Lemma 3.5.

Let us note that although the tilded operators are in general different than X'_A, X'_B and Z'_B, it turns out that they act in the same way when applied to $|\psi'\rangle$. Let us take the case of even m, where X'_B and Z'_B have to be regularised. We have that:

$$\widetilde{X}_B|\psi'\rangle = X'_B|\psi'\rangle, \qquad \widetilde{Z}_B|\psi'\rangle = Z'_B|\psi'\rangle. \tag{3.30}$$

This result is very important in order to apply the relations derived from the SOS about operators X'_B and Z'_B to operators $\widetilde{X}_B$ and $\widetilde{Z}_B$ appearing in the isometry. 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 [BP15]

$$\begin{aligned} \|(\widetilde{X}_B - X'_B)|\psi'\rangle\| &= \|(\mathbb{I} - \widetilde{X}_B^\dagger X'_B)|\psi'\rangle\| = \|(\mathbb{I} - |X'_B|)|\psi'\rangle\| \\ &= \|(\mathbb{I} - |X'_A X'_B|)|\psi'\rangle\| \leq \|(\mathbb{I} - X'_A X'_B)|\psi'\rangle\| = 0, \end{aligned} \tag{3.31}$$

where the first and the second equalities stem from the fact that $\widetilde{X}_B$ is unitary and from its definition, respectively. The third equality is a consequence of the fact that 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 equation (3.28).

Before we proceed let us make some remarks about notation. We use symbol C when we write a property or equation that is valid for both Alice and Bob's operators $C = A, B$. Note also that in some of the following expressions operators might be indexed by any integer (not just from the set $\{1, \ldots, m\}$), and in those cases we use the notation $C_{m+i} = -C_i$ and $C_{-i} = -C_{m-i}$. The intuition for this notation can be found on the Bloch sphere representation of the measurements (3.1), where we can see that if one would draw the next measurement after C_m, and note it as C_{m+1} it would be parallel to $-C_1$, and similarly for any C_{m+i}.

Lemma 3.3. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ be the pure state and the measurements realising the maximal quantum violation of the chained Bell inequalities. Then, the following identities are true:*

$$A'_i|\psi'\rangle = \frac{B'_i + B'_{i-1}}{2\cos(\pi/2m)}|\psi'\rangle \equiv B'_{i-1,i}|\psi'\rangle \tag{3.32}$$

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

$$(\alpha_i C_j + \beta_i C_{i+j} + \gamma_i C_{i+j+1})|\psi'\rangle = 0 \tag{3.33}$$

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

$$(A'_i B'_i - A'_{i+1} B'_{i+1})|\psi'\rangle = 0 \tag{3.34}$$

$$(A'_i B'_{i-1} - A'_{i+1} B'_i)|\psi'\rangle = 0 \tag{3.35}$$

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

Proof. From the fact that $|\psi'\rangle$ and A'_i and B'_i violate the chained Bell inequality maximally it follows that $\langle\psi|(B_m^{\max}\mathbb{I} - \mathcal{B}_m)|\psi'\rangle = 0$. Now, the first SOS decomposition (3.7) for the operator $B_m^{\max}\mathbb{I} - \mathcal{B}_m$ implies equations (3.32) and (3.33), while the second one implies equations (3.34) and (3.35) □

Lemma 3.4. *Let* $\{|\psi'\rangle, A'_i, B'_i\}$ *be the pure state and the measurements realising the maximal quantum violation of the chained Bell inequalities. Then, the following relations are true:*

$$\{A'_1, A'_{\frac{m}{2}+1}\}|\psi'\rangle = 0 \tag{3.36}$$

for even m, *and*

$$\{A'_1, A'_{\frac{m+1}{2}} + A'_{\frac{m+3}{2}}\}|\psi'\rangle = 0 \tag{3.37}$$

for odd m.

Proof. We prove the even and odd m cases separately.

Even number of measurements. Let us begin by noting that by setting $j = k - i$ with $k = 1, \ldots, m$ in (3.33), one obtains

$$(\alpha_i C_{k-i} + \beta_i C_k + \gamma_i C_{k+1})|\psi'\rangle = 0. \tag{3.38}$$

On the other hand, by shifting $i \to m - i - 1$ and setting $j = k + i + 1$, we arrive at

$$(\alpha_{m-i-1} C_{k+i+1} + \beta_{m-i-1} C_{k+m} + \gamma_{m-i-1} C_{k+m+1})|\psi'\rangle = 0, \tag{3.39}$$

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

$$(\alpha_i C_{k+i+1} + \gamma_i C_k + \beta_i C_{k+1})|\psi'\rangle = 0. \tag{3.40}$$

After summing equations (3.38) and (3.40) and performing some straightforward manipulations we finally obtain

$$(C_{k-i} + C_{k+i+1})|\psi'\rangle = \xi_i C_{k,k+1}|\psi'\rangle, \tag{3.41}$$

where we denoted $\xi_i = 2\cos[(2i+1)\pi/2m]$ and $C_{k,k+1} = (C_k+C_{k+1})/[2\cos(\pi/2m)]$. Finally, setting $k = 0$ in equation (3.40) and $k = m$ in equation (3.38) and subtracting the resulting equations one from another we have

$$(C_{i+1} - C_{m-i})|\psi'\rangle = \xi_i C_{1,-m}|\psi'\rangle, \tag{3.42}$$

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

Having all these auxiliary identities at hand, we are now in position to prove equation (3.36). To this end, we first rewrite its left-hand side as

$$\begin{aligned}(A'_1 A'_{\frac{m}{2}+1} + A'_{\frac{m}{2}+1}A'_1)|\psi'\rangle &= \left(A'_1 B'_{\frac{m}{2},\frac{m}{2}+1} + A'_{\frac{m}{2}+1}B'_{1,-m}\right)|\psi'\rangle \\ &= \frac{1}{\xi_{\frac{m}{2}-1}}\left[A'_1(B'_1+B'_m) + A'_{\frac{m}{2}+1}(B'_{\frac{m}{2}} - B'_{\frac{m}{2}+1})\right]|\psi'\rangle,\end{aligned} \tag{3.43}$$

where the first equality was obtained with the aid of the identity (3.32) for $i = m/2+1$, while the second one follows from equations (3.41) and (3.42). Then, the formulas (3.34) and (3.35) imply that

$$(A'_1 B'_1 - A'_{j+1}B'_{j+1})|\psi'\rangle = \sum_{i=1}^{j}(A'_i B'_i - A'_{i+1}B'_{i+1})|\psi'\rangle = 0 \tag{3.44}$$

and

$$(A'_1 B'_m + A'_{j+1}B'_j)|\psi'\rangle = \sum_{i=1}^{j}(A'_i B'_{i-1} - A'_{i+1}B'_i)|\psi'\rangle = 0 \tag{3.45}$$

hold for any $j = 1,\ldots,m$. After setting $j = m/2$ in the latter identities and inserting them into (3.43) we eventually obtain (3.36).

Odd number of measurements. Before passing to the anticommutation relation (3.37), 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 equation (3.40) and add the resulting equation to equation (3.38), obtaining

$$(C_{k+i} + C_{k-i})|\psi'\rangle = -2\frac{\beta_i}{\alpha_i}C_k - \frac{\gamma_i}{\alpha_i}(C_{k-1}+C_{k+1})|\psi'\rangle. \tag{3.46}$$

Then, setting $i = 1$ and shifting $j \to j-1$ in (3.33) we arrive at

$$(C_{j+1} + C_{j-1})|\psi'\rangle = 2\cos\left(\frac{\pi}{m}\right)C_j|\psi'\rangle, \tag{3.47}$$

which after being plugged into expression (3.46) gives rise to the following identity

$$(C_{k+i} + C_{k-i})|\psi'\rangle = \zeta_i C_k|\psi'\rangle, \tag{3.48}$$

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

Then, by setting $j = (m-1)/2$ in equations (3.44) and (3.45) and adding the resulting equations we obtain

$$A'_1(B'_1 + B'_m)|\psi'\rangle = A'_{\frac{m+1}{2}}(B'_{\frac{m+1}{2}} - B'_{\frac{m-1}{2}})|\psi'\rangle, \tag{3.49}$$

which can be further simplified by using equation (3.48) with $i = (m-1)/2$ and $k = m$, giving

$$A'_1(B'_1 + B'_m)|\psi'\rangle = \zeta_{\frac{m-1}{2}} A'_{\frac{m+1}{2}} B'_m|\psi'\rangle. \tag{3.50}$$

Analogously, by setting $j = (m+1)/2$ in equations (3.44) and (3.45) and adding them, one obtains

$$A'_1(B'_1 + B'_m)|\psi'\rangle = A'_{\frac{m+3}{2}}(B'_{\frac{m+3}{2}} - B'_{\frac{m+1}{2}})|\psi'\rangle, \tag{3.51}$$

which, after application of equation (3.48) with $i = (m-1)/2$ and $k = m+1$, further simplifies to

$$A'_1(B'_1 + B'_m)|\psi'\rangle = -\zeta_{\frac{m-1}{2}} A'_{\frac{m+3}{2}} B'_1|\psi'\rangle. \tag{3.52}$$

Now, we can rewrite the left-hand side of the anticommutation relation (3.37) as

$$\begin{aligned}\left\{A'_1, A'_{\frac{m+1}{2}} + A'_{\frac{m+3}{2}}\right\}|\psi'\rangle &= \tfrac{1}{2\cos\frac{\pi}{2m}} \Big[A'_1(B'_{\frac{m-1}{2}} + 2B'_{\frac{m+1}{2}} + B'_{\frac{m+3}{2}}) + \\ &\qquad (A'_{\frac{m+1}{2}} + A_{\frac{m+3}{\prime}2})(B'_1 - B'_m)\Big]|\psi'\rangle \\ &= \tfrac{1}{2\cos\frac{\pi}{2m}} \Big[A'_1\left(B'_{\frac{m-1}{2}} + B'_{\frac{m+3}{2}} + 2\frac{B'_1 + B'_m}{\zeta_{(m-1)/2}}\right) + \\ &\qquad (A'_{\frac{m+1}{2}} + A'_{\frac{m+3}{2}})(B'_1 - B'_m)\Big]|\psi'\rangle,\end{aligned} \tag{3.53}$$

where first equality stems from equation (3.32) and to obtain the second one we have utilised equation (3.48) with $i = (m-1)/2$ and $k = (m+1)/2$. Then, expressions (3.50) and (3.52) lead us to

$$\begin{aligned}\left\{A'_1, A'_{\frac{m+1}{2}} + A'_{\frac{m+3}{2}}\right\}|\psi'\rangle = \frac{1}{2\cos(\pi/2m)}\Big(A'_1 B'_{\frac{m-1}{2}} + A'_1 B'_{\frac{m+3}{2}} + \\ A'_{\frac{m+1}{2}} B'_1 - A'_{\frac{m+3}{2}} B'_m\Big)|\psi'\rangle.\end{aligned} \tag{3.54}$$

Exploiting once more (3.48) one obtains the following equalities

$$A'_1|\psi'\rangle = \frac{1}{\zeta_{\frac{m-1}{2}}}(A'_{\frac{m+1}{2}} - A'_{\frac{m+3}{2}})|\psi'\rangle, \quad B'_1|\psi'\rangle = \frac{1}{\zeta_{\frac{m-1}{2}}}(B'_{\frac{m+1}{2}} - B'_{\frac{m+3}{2}})|\psi'\rangle, \tag{3.55}$$

and

$$B'_m|\psi'\rangle = \frac{1}{\zeta_{\frac{m-1}{2}}}(B'_{\frac{m+1}{2}} - B'_{\frac{m-1}{2}})|\psi'\rangle, \tag{3.56}$$

whose application to equation (3.54) allows one to rewrite it as

$$\left\{A'_1, A'_{\frac{m+1}{2}} + A'_{\frac{m+3}{2}}\right\}|\psi'\rangle = \frac{1}{2\zeta_{\frac{m-1}{2}}\cos\frac{\pi}{2m}}\Big(A'_{\frac{m+1}{2}}B'_{\frac{m-1}{2}} - A'_{\frac{m+3}{2}}B'_{\frac{m+1}{2}} + A'_{\frac{m+1}{2}}B'_{\frac{m+1}{2}} - A'_{\frac{m+3}{2}}B'_{\frac{m+3}{2}}\Big)|\psi'\rangle. \tag{3.57}$$

To complete the proof it suffices to make use of the equalities (3.34) and (3.35) with $j = (m+1)/2$. □

Lemma 3.5. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ realise the maximal quantum violation of the chained Bell inequality. Then, for even m:*

$$A'_i|\psi'\rangle = \left(s_iA'_{\frac{m}{2}+1} + c_iA'_1\right)|\psi'\rangle, \tag{3.58}$$

$$B'_i|\psi'\rangle = \left(s'_iB'_{\frac{m}{2},\frac{m}{2}+1} + c'_iB'_{1,-m}\right)|\psi'\rangle, \tag{3.59}$$

while for odd m:

$$A'_i|\psi'\rangle = \left\{s_iA'_{\frac{m+1}{2},\frac{m+3}{2}} + c_iA'_1\right\}|\psi'\rangle, \tag{3.60}$$

$$B'_i|\psi'\rangle = \left\{s'_iB'_{\frac{m+1}{2}} + c'_iB'_{1,-m}\right\}|\psi'\rangle, \tag{3.61}$$

are valid for any $i = 1, \ldots, m$. Symbols s_i, c_i, s'_i and c'_i are defined in equation (3.6).

Proof. **Even number of measurements.** By setting $k = 1+m/2$ and shifting $i \to 1-i+m/2$ in equation (3.48) one obtains

$$(C_i - C_{2-i})|\psi'\rangle = \zeta_{\frac{m}{2}+1-i}C_{\frac{m}{2}+1}|\psi'\rangle. \tag{3.62}$$

for $i = 1, \ldots, m/2$, where we have additionally exploited the fact that $C_{m+i} = -C_i$ and $C_{-i} = -C_{m-i}$ for any i. To prove equation (3.62) for $i = m/2 +$

$1, \ldots, m/2$ one has to use (3.38) but coefficients α_i, β_i and γ_i are not defined for $i < 0$. However, once (3.62) is derived for $i < m/2 + 1$, it is easy to note that the cases when $i > m/2 + 1$ are already contained in the proof. This is due to the fact that any expression obtained when $i > m/2 + 1$ is the same as the expression proved for $m + 2 - i < m/2 + 1$.
On the other hand, fixing $k = 1$ and shifting $i \to i - 1$ in (3.48), one can deduce the following equality

$$(C_i + C_{2-i})|\psi'\rangle = \zeta_{i-1} C_1 |\psi'\rangle, \tag{3.63}$$

with $i = 2, \ldots m$. For $i = 1$, the equation is trivial. Adding equations (3.62) and (3.63) and recalling that $\zeta_i = 2\cos(i\pi/m)$ one obtains equation (3.58).

In order to prove the second identity (3.59), we fix $k = m/2$ and shift $i \to m/2 - i$ in equation (3.41) which leads us to

$$(C_i + C_{m-i+1})|\psi'\rangle = \xi_{\frac{m}{2}-i} C_{\frac{m}{2}, \frac{m}{2}+1} |\psi'\rangle. \tag{3.64}$$

This equation is satisfied for all $i = 1, \ldots, m$, but it could formally be derived only when $i < m/2$. The cases $i = m/2, m/2+1$ are trivially satisfied. Similarly to the discussion following equation (3.62) it is easy to check that for every $i > m/2 + 1$ equation (3.64) is the same as for the case $m + 1 - i < m/2$, which has been formally proven.

Now we note that by shifting $i \to i - 1$ in (3.42), one obtains the following equation

$$(C_i - C_{m-i+1})|\psi'\rangle = \xi_{i-1} C_{1,-m} |\psi'\rangle, \tag{3.65}$$

which when combined with (3.64) directly implies (3.59), completing the proof.

Odd number of measurements. First in equation (3.41) we fix $k = (m + 1)/2$ and shift $i \to (m + 1)/2 - i$ to get

$$(C_i + C_{m+2-i})|\psi'\rangle = \xi_{\frac{m+1}{2}-i} C_{\frac{m+1}{2}, \frac{m+3}{2}} |\psi'\rangle. \tag{3.66}$$

This equation is consistent for all $i = 1, \ldots, m$, with the clarification exactly the same as in the discussion following equation (3.64). Next step is to plug $k = 1$ and $i \to i - 1$ in (3.48) which together with $C_{2-i} = -C_{m+2-i}$ gives

$$(C_i - C_{m+2-i})|\psi'\rangle = \zeta_{i-1} C_1 |\psi'\rangle \tag{3.67}$$

By adding equations (3.66) and (3.67) and using some elementary trigonometric identities we obtain (3.60). We proceed by fixing $k = (m + 1)/2$ and shifting $i \to (m + 1)/2 - i$ in (3.48) to obtain

$$(C_i + C_{m+1-i})|\psi'\rangle = \zeta_{\frac{m+1}{2}-i} C_{\frac{m+1}{2}} |\psi'\rangle, \tag{3.68}$$

satisfied for all $i = 1, \ldots, m$ in the same way as equation (3.62). To get (3.61) and complete the proof to equation (3.68) we add

$$(C_i - C_{m+1-i})|\psi'\rangle = \xi_{i-1} C_{1,-m}|\psi'\rangle \tag{3.69}$$

which is obtained by shifting $i \to i-1$ in (3.42). □

3.3.4. Self-test

Equipped with the results of Section 3.3.3, we are ready to prove our first main result: self-testing in the ideal case. We prove it for even m for clarity (the proof for odd m can be done in an analogous way).

Theorem 3.6. *Let $\{|\psi'\rangle, A_i', B_i'\}$ be the state and the measurements maximally violating the chained Bell inequality (3.1). Then the unitary operation Φ defined in Figure 3.2 is such that for any pair $i, j = 1, \ldots, m$*

$$\Phi(A_i' B_j' |\psi'\rangle|00\rangle) = |\varphi\rangle A_i B_j |\phi^+\rangle, \tag{3.70}$$

$$\Phi(A_i'|\psi'\rangle|00\rangle) = |\varphi\rangle A_i|\phi^+\rangle, \qquad \Phi(B_j'|\psi'\rangle|00\rangle) = |\varphi\rangle B_j|\phi^+\rangle, \tag{3.71}$$

$$\Phi(|\psi'\rangle|00\rangle) = |\varphi\rangle|\phi^+\rangle, \tag{3.72}$$

where $|\varphi\rangle$ is the junk state, $|\phi^+\rangle$ is the two-qubit maximally entangled state, and A_i and B_i are given by expression (3.6).

Proof. Let us first consider equation (3.70). Owing to the linearity of Φ in both Alice's and Bob's measurements and to the fact that for even m (see Lemma 3.5 in 3.3.3):

$$A_i'|\psi'\rangle = \left(s_i X_A' + c_i Z_A'\right)|\psi'\rangle, \qquad B_i'|\psi'\rangle = \left(s_i' X_B' + c_i' Z_B'\right)|\psi'\rangle, \tag{3.73}$$

the left-hand side of (3.70) can be rewritten as

$$\begin{aligned} \Phi(A_i' B_j'|\psi'\rangle|00\rangle) \quad = \quad & s_i s_j' \Phi(X_A' X_B'|\psi'\rangle|00\rangle) + s_i c_j' \Phi(X_A' Z_B'|\psi'\rangle|00\rangle) \\ & + c_i s_j' \Phi(Z_A' X_B'|\psi'\rangle|00\rangle) + c_i c_j' \Phi(Z_A' Z_B'|\psi'\rangle|00\rangle). \end{aligned} \tag{3.74}$$

Then, it follows from equations (3.28) and (3.29) 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

$$\begin{aligned} \Phi(|\psi'\rangle|00\rangle) = \frac{1}{4}\big[& (\mathbb{I} + Z_A')(\mathbb{I} + \widetilde{Z}_B)|\psi'\rangle|00\rangle + X_A'(\mathbb{I} - Z_A')(\mathbb{I} + \widetilde{Z}_B)|\psi'\rangle|10\rangle \\ & + \widetilde{X}_B(\mathbb{I} + Z_A')(\mathbb{I} - \widetilde{Z}_B)|\psi'\rangle|01\rangle + X_A'\widetilde{X}_B(\mathbb{I} - Z_A')(\mathbb{I} - \widetilde{Z}_B)|\psi'\rangle|11\rangle\big]. \end{aligned} \tag{3.75}$$

Exploiting equations (3.28) and (3.30) 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 $(\mathbb{I}+Z'_A)$ and $(\mathbb{I}-Z'_A)$ are projectors onto orthogonal subspaces, one finds that the terms in expression (3.75) containing the ancillary vectors $|01\rangle$ and $|10\rangle$ simply vanish, and the whole expression simplifies to

$$\Phi(|\psi'\rangle|00\rangle) = \frac{1}{4}\big[(\mathbb{I}+Z'_A)^2|\psi'\rangle|00\rangle + X'_A\widetilde{X}_B(\mathbb{I}-Z'_A)^2|\psi'\rangle|11\rangle\big]. \tag{3.76}$$

Using then the fact that $(\mathbb{I}\pm Z'_A)^2 = 2(\mathbb{I}\pm Z'_A)$, the anticommutation relation (3.29) and the identities (3.28) and (3.30), we finally obtain

$$\Phi(|\psi'\rangle|00\rangle) = |\varphi\rangle|\phi^+\rangle \tag{3.77}$$

with $|\varphi\rangle = (1/2\sqrt{2})(\mathbb{I}+Z'_A)^2|\psi'\rangle$, which is exactly (3.72).

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

$$\begin{aligned}\Phi(X'_AZ'_B|\psi'\rangle|00\rangle) \quad = \quad & \frac{1}{4}\big[(\mathbb{I}+Z'_A)(\mathbb{I}+\widetilde{Z}_B)X'_AZ'_B|\psi'\rangle|00\rangle \\ & +X'_A(\mathbb{I}-Z'_A)(\mathbb{I}+\widetilde{Z}_B)X'_AZ'_B|\psi'\rangle|10\rangle \\ & +\widetilde{X}_B(\mathbb{I}+Z'_A)(\mathbb{I}-\widetilde{Z}_B)X'_AZ'_B|\psi'\rangle|01\rangle \\ & +X'_A\widetilde{X}_B(\mathbb{I}-Z'_A)(\mathbb{I}-\widetilde{Z}_B)X'_AZ'_B|\psi'\rangle|11\rangle\big].\end{aligned} \tag{3.78}$$

Exploiting the properties (3.28) and (3.30), the anticommutation relation (3.29), and the fact that $(\mathbb{I}+Z'_A)(\mathbb{I}-Z'_A)=0$, one can prove that the terms in (3.78) containing kets $|00\rangle$ and $|11\rangle$ are zero, and the whole expression reduces to

$$\Phi(X'_AZ'_B|\psi'\rangle|00\rangle) \quad = \quad \frac{1}{4}\left[(\mathbb{I}+Z'_A)^2|\psi'\rangle|10\rangle + X'_AZ'_A\widetilde{X}_B(\mathbb{I}-Z'_A)^2|\psi'\rangle|01\rangle\right]. \tag{3.79}$$

By applying then equation (3.28) and the anticommutation relation (3.29) in the second term of (3.79), one can rewrite it as

$$\Phi(X'_AZ'_B|\psi'\rangle|00\rangle) = |\varphi\rangle X_AZ_B|\phi^+\rangle. \tag{3.80}$$

After plugging equations (3.77) and (3.80) into equation (3.74) 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

$$\begin{aligned}\Phi(A'_iB'_j|\psi'\rangle|00\rangle) \quad = \quad & s_is'_i|\varphi\rangle X_AX_B|\phi^+\rangle + s_ic'_i|\varphi\rangle X_AZ_B|\phi^+\rangle \\ & +c_is'_i|\varphi\rangle Z_AX_B|\phi^+\rangle + c_ic'_i|\varphi\rangle Z_AZ_B|\phi^+\rangle,\end{aligned} \tag{3.81}$$

which by virtue of the formulas (3.6) is exactly equation (3.70).

Let us now prove equations (3.71). From the the linearity of Φ and equation (3.73), 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

$$\Phi(X_A'|\psi'\rangle|00\rangle) = |\varphi\rangle X_A|\phi^+\rangle, \qquad \Phi(Z_A'|\psi'\rangle|00\rangle) = |\varphi\rangle Z_A|\phi^+\rangle, \tag{3.82}$$

which when plugged into (3.82) leads, in virtue of (3.73), to the first part of expression (3.71). The second part of the same equation can be proven in exactly the same way. □

Corollary. *An important corollary following directly from Theorem 3.6 is that the probability distribution* $\{P(a,b|i,j)\}$ *with*

$$P(a,b|i,j) = \langle\psi'|M_{a|i}\otimes N_{b|j}|\psi'\rangle \tag{3.83}$$

being the conditional probability of obtaining the outcomes a *and* b *upon performing the* i*th and* j*th measurement, respectively, is unique. In other words, there is no other probability distribution maximally violating inequality (3.1) different than the one above.*

Let us also notice that in order to prove the uniqueness of correlations maximally violating the chained Bell inequality one needs only the conditions (3.71) and (3.72); the conditions (3.70) are superfluous. This is because

$$\begin{aligned} \langle\psi'|A_i'\otimes B_j'|\psi'\rangle &= (\langle 00|\langle\psi'|A_i')\Phi^\dagger\Phi(B_j'|\psi'\rangle|00\rangle) \\ &= \langle\phi^+|A_i\otimes B_j|\phi^+\rangle, \end{aligned} \tag{3.84}$$

where the first equality follows from the fact that Φ is unitary and and second from equations (3.71) and (3.72).

3.4. Robustness

For practical purposes, it is important to estimate the robustness of self-testing procedures, since it is impossible to actually reach the maximal violation of a Bell inequality in any realistic situation, due to experimental imperfections. 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.

Here we study how robust is the above self-testing procedure based on the chained Bell inequalities. Assuming that the physical state $|\psi'\rangle$ and the physical measurements A'_i and B'_i violate the chained Bell inequality by $B_m^{\max} - \varepsilon$ 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.

3.4.1. Approximate relations from the sum-of-squares decompositions

Let us begin by noticing that now $\langle\psi'|(B_m^{\max}\mathbb{I} - \mathcal{B}_{\mathrm{m}})|\psi'\rangle = \varepsilon$, and therefore the exact relations (3.28), (3.29) and (3.30) do not hold anymore. In this section, we derive their approximate versions. First, we show in Lemma 3.7 that

$$\|(X'_A - X'_B)|\psi'\rangle\| \leq \sqrt{\varepsilon_1(m)}, \qquad \|(Z'_A - Z'_B)|\psi'\rangle\| \leq \sqrt{\varepsilon_1(m)}, \tag{3.85}$$

where $\varepsilon_1 = \varepsilon/\cos(\pi/2m)$. Clearly, for any m, $\varepsilon_1(m) \leq \sqrt{2}$ and $\varepsilon_1(m) \to 0$ for $\varepsilon \to 0$. Then, we find the following approximate anticommutation relations in Lemma 3.8:

$$\|\{X'_A, Z'_A\}|\psi'\rangle\| \leq \sqrt{2\varepsilon_1(m)} + \frac{1}{\xi_{m/2-1}}\left(\frac{4\sqrt{\epsilon_1(m)}}{\alpha_{m/2-1}} + m\sqrt{2\varepsilon_2(m)}\right) = \omega_{\mathrm{ev}}(m), \tag{3.86}$$

where $\xi_i = 2\cos(2i+1)\pi/2m$, α_i is defined in Lemma 3.1, and ε_1 and ε_2 are given in Lemma 3.7. In what follows we drop the dependence of ε_1 and ε_2 on m. Moreover, we can follow the same reasoning as in (3.31) to relate the operators to their regularised versions:

$$\|(\widetilde{X}'_B - X'_B)|\psi'\rangle\| \leq \sqrt{\varepsilon_1(m)}, \qquad \|(\widetilde{Z}'_B - Z'_B)|\psi'\rangle\| \leq \sqrt{\varepsilon_1(m)}. \tag{3.87}$$

Let us begin with the approximate version of Lemma 3.3.

Lemma 3.7. *Let $|\psi'\rangle$ and $\{A'_i, B'_i\}$ be the state and the measurements violating the chained Bell inequality by $B_m^{\max} - \epsilon$. Then, the following relations are satisfied:*

$$\|(A'_i - B'_{i-1,i})|\psi'\rangle\| \leq \sqrt{\frac{\varepsilon}{\cos(\pi/2m)}} \equiv \sqrt{\epsilon_1} \tag{3.88}$$

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

$$\|(\alpha_i B'_j + \beta_i B'_{i+j} + \gamma_i B'_{i+j+1})|\psi'\rangle\| \leq \sqrt{\epsilon_1} \tag{3.89}$$

for $i = 1, \dots, m-2$ and $j = 1, \dots, m$, and

$$\|(A'_i \otimes B'_i - A'_{i+1} \otimes B'_{i+1})|\psi'\rangle\| \leq \sqrt{8m\cos\frac{\pi}{2m}\epsilon} \equiv \sqrt{m\varepsilon_2}, \tag{3.90}$$

$$\|(A'_i \otimes B'_{i-1} - A'_{i+1} \otimes B'_i)|\psi'\rangle\| \leq \sqrt{m\varepsilon_2} \tag{3.91}$$

for $i = 1, \dots, m$.

Proof. All equations follow directly from the SOS decompositions. When a chained Bell inequality is violated by the amount $2m\cos[\pi/2m] - \epsilon$, it follows that $\sum_i \langle\psi'|P_i^2|\psi'\rangle = \epsilon$ and consequently $||P_i|\psi'\rangle|| \leq \sqrt{\epsilon}$ for all i. The expressions given by equations (3.88) and (3.89) are identified in the first degree SOS decomposition (3.7) (note the explanation after the equation), while the expressions bounded in equations (3.90) and (3.91) are part of the second degree SOS decomposition (3.23). □

We can then prove the approximate version of Lemma 3.4 .

Lemma 3.8. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ be the state and the measurements violating the chained Bell inequality by $B_m^{\max} - \varepsilon$. Then, the following approximate anticommutation relations are true*

$$\|\{A'_1, A'_{\frac{m}{2}+1}\}|\psi'\rangle\| \leq \sqrt{2\varepsilon_1} + \frac{1}{\xi_{m/2-1}}\left(\frac{4\sqrt{\epsilon_1}}{\alpha_{m/2-1}} + m\sqrt{2\varepsilon_2}\right) = \omega_{\text{ev}} \tag{3.92}$$

for even m, and

$$\begin{aligned}\|\{A'_1, A'_{\frac{m+1}{2}} + A'_{\frac{m+3}{2}}\}|\psi'\rangle\| \;\leq\;& 2\sqrt{\varepsilon_1}m\left(\frac{\sqrt{2}}{\zeta_{(m-1)/2}} + \sqrt{m-1}\right) + \sqrt{\varepsilon_1}(1+\sqrt{2}) \\ &+ \frac{3\sqrt{\varepsilon_1}}{\cos\frac{\pi}{2m}\alpha_{(m-1)/2}\zeta_{(m-1)/2}}\left(2 + \frac{\gamma_{(m-1)/2}}{\alpha_1}\right) = \omega_{\text{odd}}\end{aligned} \tag{3.93}$$

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

Proof. The proof goes along the same lines as that of Lemma 3.4, 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 m separately.

Even number of measurements. We first need to prove the approximate versions of the identities (3.41) and (3.42). By substituting $j = k - i$ in (3.89) we obtain

$$\|(\alpha_i C_{k-i} + \beta_i C_k + \gamma_i C_{k+1})|\psi'\rangle\| \leq \sqrt{\varepsilon_1}. \tag{3.94}$$

Then, by shifting $i \to m - i - 1$ and setting $j = k + i + 1$ in (3.89), we have

$$\|(\alpha_i C_{k+i+1} + \gamma_i C_k + \beta_i C_{k+1})|\psi'\rangle\| \leq \sqrt{\varepsilon_1}. \tag{3.95}$$

Both inequalities imply

$$\|(C_{k-i} + C_{k+i+1} - \xi_i C_{k,k+1})|\psi'\rangle\| \leq \frac{2\sqrt{\varepsilon_1}}{\alpha_i} \tag{3.96}$$

for any $k = 1, \ldots, m$ and $i = 1, \ldots, m-2$. The cases where $i = m-1$ or $i = m$ are trivial because they represent the definition of $C_{k,k+1}$. Then, by using (3.94) with $k = m$ and (3.95) with $k = 0$, one can prove the following inequality

$$\|(C_{i+1} - C_{m-i} - \xi_i C_{1,-m})|\psi'\rangle\| \leq \frac{2\sqrt{\varepsilon_1}}{\alpha_i} \tag{3.97}$$

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

$$\begin{aligned} \|\{A'_1, A'_{\frac{m}{2}+1}\}|\psi'\rangle\| &= \|(A'_1 A'_{\frac{m}{2}+1} + A'_{\frac{m}{2}+1} A'_1)|\psi'\rangle\| \\ &\leq \|(A'_1 B'_{\frac{m}{2},\frac{m}{2}+1} + A'_{\frac{m}{2}+1} B'_{1,-m})|\psi'\rangle\| + \sqrt{2\varepsilon_1}, \end{aligned} \tag{3.98}$$

which with the aid of (3.96) with $k = m/2$ and $i = m/2 - 1$ and (3.97) with $i = m/2 - 1$, can be further upper bounded as

$$\begin{aligned} \left\|\{A'_1, A'_{\frac{m}{2}+1}\}|\psi'\rangle\right\| &\leq \frac{1}{\xi_{m/2-1}} \left\|\left[A'_1(B'_1 + B'_m) + A'_{\frac{m}{2}+1}(B'_{\frac{m}{2}} - B'_{\frac{m}{2}+1})\right]|\psi'\rangle\right\| \\ &\quad + \frac{1}{\xi_{m/2-1}} \frac{4\sqrt{\varepsilon_1}}{\alpha_{m/2-1}} \\ &\leq \frac{1}{\xi_{m/2-1}} \left\|(A'_1 B'_1 - A'_{\frac{m}{2}+1} B'_{\frac{m}{2}+1})|\psi'\rangle\right\| \\ &\quad + \frac{1}{\xi_{m/2-1}} \left\|(A'_1 B'_m + A'_{\frac{m}{2}+1} B'_{\frac{m}{2}})|\psi'\rangle\right\| \\ &\quad + \frac{1}{\xi_{m/2-1}} \frac{4\sqrt{\varepsilon_1}}{\alpha_{m/2-1}}. \end{aligned} \tag{3.99}$$

To upper bound the above two terms, we will use approximate versions of equations (3.44) and (3.45) First, it follows from the SOS decomposition that for any $j = 1, \ldots, m$:

$$\sum_{i=1}^{j} \left\|(A'_i B'_i - A'_{i+1} B'_{i+1})|\psi'\rangle\right\|^2 \leq m\varepsilon_2, \tag{3.100}$$

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

$$\begin{aligned}\left\|(A_1'B_1'-A_{j+1}'B_{j+1}')|\psi'\rangle\right\| &= \left\|\sum_{i=1}^{j}(A_i'B_i'-A_{i+1}'B_{i+1}')|\psi'\rangle\right\| \\ &\leq \sum_{i=1}^{j}\left\|(A_i'B_i'-A_{i+1}'B_{i+1}')|\psi'\rangle\right\| \\ &\leq \sqrt{j}\sqrt{\sum_{i=1}^{j}\left\|(A_i'B_i'-A_{i+1}'B_{i+1}')|\psi'\rangle\right\|^2} \\ &\leq \sqrt{jm\varepsilon_2}. \end{aligned} \tag{3.101}$$

Analogously, the SOS decomposition (3.23) implies that

$$\sum_{i=1}^{j}\left\|(A_i'B_{i-1}'-A_{i+1}'B_i')|\psi'\rangle\right\|^2 \leq \sqrt{m\varepsilon_2}, \tag{3.102}$$

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

$$\left\|(A_1'B_m'+A_{j+1}'B_j')|\psi'\rangle\right\| = \sum_{i=1}^{j}\left\|(A_i'B_{i-1}'-A_{i+1}'B_i')|\psi'\rangle\right\| \leq \sqrt{jm\varepsilon_2}. \tag{3.103}$$

Substituting $j = m/2$ and applying both inequalities (3.101) and (3.103) to (3.99) one finally obtains (3.92).

Odd number of measurements. We first prove the following inequality

$$\|(C_{k-i}+C_{k+i}-\zeta_i C_k)|\psi'\rangle\| \leq \left(2+\frac{\gamma_i}{\alpha_1}\right)\frac{\sqrt{\varepsilon_1}}{\alpha_i} \tag{3.104}$$

for any $i = 1,\ldots,m-2$. Then, from inequalities (3.101) and (3.103) with $j=(m-1)/2$, and inequality (3.104) for $i=(m-1)/2$ and $k=m$, one obtains

$$\left\|\left[A_1'(B_1'+B_m')-\zeta_{\frac{m-1}{2}}A_{\frac{m+1}{2}}'B_m'\right]|\psi'\rangle\right\| \leq \sqrt{2m(m-1)\varepsilon_2}+\varepsilon', \tag{3.105}$$

where we denoted

$$\varepsilon' = \frac{\sqrt{\varepsilon_1}}{\alpha_{(m-1)/2}}\left(2+\frac{\gamma_{(m-1)/2}}{\alpha_1}\right). \tag{3.106}$$

Analogously, from inequalities (3.101) and (3.103) with $j = (m+1)/2$ and inequality (3.104) for $i = (m-1)/2$ and $k = m+1$, one obtains

$$\left\| \left[A'_1(B'_1 + B'_m) + \zeta_{\frac{m-1}{2}} A'_{\frac{m+3}{2}} B'_m \right] |\psi'\rangle \right\| \quad \leq \quad \sqrt{2m(m-1)\varepsilon_2} + \varepsilon'. \tag{3.107}$$

We can then upper bound

$$\begin{aligned}
\left\| \{A'_1, A'_{\frac{m+1}{2}} + A'_{\frac{m+3}{2}}\}|\psi'\rangle \right\| \quad \leq \quad & \frac{1}{2\cos(\frac{\pi}{2m})} \Big\| [A'_1(B'_{\frac{m-1}{2}} + 2B'_{\frac{m+1}{2}} + B'_{\frac{m+3}{2}}) \\
& \qquad + (A'_{\frac{m+1}{2}} + A'_{\frac{m+3}{2}})(B'_1 - B'_m)]|\psi'\rangle \Big\| \\
& + \sqrt{\varepsilon_1}(1+\sqrt{2}) \\
\leq \quad & \frac{1}{2\cos(\frac{\pi}{2m})} \Big\| [A'_1 \left(B'_{\frac{m-1}{2}} + B'_{\frac{m+3}{2}} + 2\frac{B'_1 + B'_m}{\zeta_{(m-1)/2}} \right) \\
& \qquad + (A'_{\frac{m+1}{2}} + A'_{\frac{m+3}{2}})(B'_1 - B'_m)]|\psi'\rangle \Big\| \\
& + \sqrt{\varepsilon_1}(1+\sqrt{2}) + \frac{\varepsilon'}{2\cos(\pi/2m)\zeta_{(m-1)/2}} \\
\leq \quad & \frac{1}{2\cos(\frac{\pi}{2m})} \Big\| \Big(A'_1 B'_{\frac{m-1}{2}} + A'_1 B'_{\frac{m+3}{2}} \\
& \qquad + A'_{\frac{m+1}{2}} B'_1 - A'_{\frac{m+3}{2}} B'_m \Big) |\psi'\rangle \Big\| \\
& + \sqrt{\varepsilon_1}(1+\sqrt{2}) + \frac{3\varepsilon'}{2\cos(\pi/2m)\zeta_{(m-1)/2}} \\
& + 2\sqrt{\varepsilon_1 m(m-1)}.
\end{aligned} \tag{3.108}$$

In the first inequality we used (3.88) twice in parallel (to exchange A'_{m+2} and A'_{m+3} with corresponding B's) and once more separately (to exchange A'_1 with $B'_{1,-m}$). To get the second inequality we used (3.104) and for the final inequality we used twice (3.107). Inequality (3.104) for $k = 1$ and $i = (m-1)/2$ gives

$$\left\| [A'_{\frac{m+1}{2}} - A'_{\frac{m+3}{2}} - \zeta_{\frac{m-1}{2}} A'_1]|\psi'\rangle \right\| \leq \varepsilon', \tag{3.109}$$

$$\left\| [B'_{\frac{m+1}{2}} - B'_{\frac{m+3}{2}} - \zeta_{\frac{m-1}{2}} B'_1]|\psi'\rangle \right\| \leq \varepsilon' \tag{3.110}$$

while for $k = m$ and $i = (m-1)/2$

$$\left\| [B'_{\frac{m+1}{2}} - B'_{\frac{m-1}{2}} - \zeta_{\frac{m-1}{2}} B'_m]|\psi'\rangle \right\| \leq \varepsilon'. \tag{3.111}$$

These three inequalities when applied to (3.108) give

$$\begin{aligned}&\left\|\{A_1',A_{\frac{m+1}{2}}'+A_{\frac{m+3}{2}}'\}|\psi'\rangle\right\|\\&\leq\frac{1}{2\cos(\frac{\pi}{2m})\zeta_{\frac{m-1}{2}}}\left\|\left(A_{\frac{m+1}{2}}'B_{\frac{m-1}{2}}'-A_{\frac{m+3}{2}}'B_{\frac{m+1}{2}}'+A_{\frac{m+1}{2}}'B_{\frac{m+1}{2}}'-A_{\frac{m+3}{2}}'B_{\frac{m+3}{2}}'\right)|\psi'\rangle\right\|\\&\quad+\sqrt{\varepsilon_1}(1+\sqrt{2})+\frac{3\varepsilon'}{\cos\frac{\pi}{2m}\zeta_{(m-1)/2}}+2\sqrt{\varepsilon_1 m(m-1)}.\end{aligned}\tag{3.112}$$

To upper bound the norm appearing on the right-hand side we use inequalities (3.90) and (3.91) with $i=(m+1)/2$ which leads us to

$$\begin{aligned}\left\|\{A_1',A_{\frac{m+1}{2}}'+A_{\frac{m+3}{2}}'\}|\psi'\rangle\right\|\ \leq\ &2\sqrt{\varepsilon_1 m}\left(\frac{\sqrt{2}}{\zeta_{(m-1)/2}}+\sqrt{m-1}\right)+\sqrt{\varepsilon_1}(1+\sqrt{2})\\&+\frac{3\sqrt{\varepsilon_1}}{\cos\frac{\pi}{2m}\alpha_{(m-1)/2}\zeta_{(m-1)/2}}\left(2+\frac{\gamma_{(m-1)/2}}{\alpha_1}\right).\end{aligned}\tag{3.113}$$

To complete the proof let us notice that both ω_{ev} and ω_{odd}, defined in equations (3.92) and (3.93) respectively, vanish when $\varepsilon\to 0$. Furthermore, the term dominating the scaling of ω_{ev} with m for large m is $4\varepsilon_1/(\xi_{m/2-1}\alpha_{m/2-1})=2\sqrt{\varepsilon}/(\sin^2(\pi/2m))$. It follows that for sufficiently large m the function $1/\sin^2(\pi/2m)$ behaves like $(4/\pi^2)m^2+1/3+O(1/m^2)$ and therefore we can conclude that ω_{ev} scales quadratically with m when m is large enough, and for small ε it behaves as $\sqrt{\varepsilon}$. After an analogous analysis one finds that ω_{odd} exhibits the same behaviour for small ε and sufficiently large m. □

Let us now prove the approximate version of Lemma 3.5.

Lemma 3.9. *Let $|\psi'\rangle$ and A_i',B_i' be a state and measurements violating the chained Bell inequalities by $B_m^{\max}-\varepsilon$. Then, for an even number of measurements:*

$$\begin{aligned}\left\|\left(A_i'-s_iA_{\frac{m}{2}+1}'-c_iA_1'\right)|\psi'\rangle\right\|&\leq g_{\mathrm{ev}}(\varepsilon,m),\\\left\|\left(B_i'-s_i'B_{\frac{m}{2},\frac{m}{2}+1}'-c_i'B_{1,-m}'\right)|\psi'\rangle\right\|&\leq h_{\mathrm{ev}}(\varepsilon,m),\end{aligned}\tag{3.114}$$

while for an odd number of measurements:

$$\begin{aligned}\left\|\left(A_i'-s_iA_{\frac{m+1}{2},\frac{m+3}{2}}'-c_iA_1'\right)|\psi'\rangle\right\|&\leq g_{\mathrm{odd}}(\varepsilon,m),\\\left\|\left(B_i'-s_i'B_{\frac{m+1}{2}}'-c_i'B_{1,-m}'\right)|\psi'\rangle\right\|&\leq h_{\mathrm{odd}}(\varepsilon,m).\end{aligned}\tag{3.115}$$

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

Proof. We will follow the proof of Lemma 3.5. We can write

$$
\begin{aligned}
&\left\|\left(A'_i - s_i A'_{\frac{m}{2}+1} - c_i A'_1\right)|\psi'\rangle\right\| \\
&= \frac{1}{2}\left\|\left(A'_i - A'_{2-i} - \zeta_{\frac{m}{2}+1-i} A'_{\frac{m}{2}+1} + A'_i + A'_{2-i} - \zeta_{i-1} A'_1\right)|\psi'\rangle\right\| \\
&\leq \frac{1}{2}\left\|\left(A'_i - A'_{2-i} - \zeta_{\frac{m}{2}+1-i} A'_{\frac{m}{2}+1}\right)|\psi'\rangle\right\| + \frac{1}{2}\left\|\left(A'_i + A'_{2-i} - \zeta_{i-1} A'_1\right)|\psi'\rangle\right\| \\
&\leq \left(1 + \frac{\gamma_{|\frac{m}{2}+1-i|}}{2\alpha_1}\right)\frac{\sqrt{\varepsilon_1}}{\alpha_{|\frac{m}{2}+1-i|}} + \left(1 + \frac{\gamma_{i-1}}{2\alpha_1}\right)\frac{\sqrt{\varepsilon_1}}{\alpha_{i-1}} = g_{\mathrm{ev}}. \qquad (3.116)
\end{aligned}
$$

The equality is just the rewritten pair of equations (3.62) and (3.63), and the first inequality is the triangle inequality followed by the bounds from equation (3.104). The absolute value appearing in $\gamma_{|\frac{m}{2}+1-i|}$ and $\alpha_{|\frac{m}{2}+1-i|}$ is justified in the discussion after equation (3.62). Note that this bound cannot be applied to the cases when $i = 1, m/2+1, m$ because for these cases the coefficients α_i and γ_i are not defined. The cases $i = 1, m/2+1$ are trivial statements and $g_{\mathrm{ev}} = 0$, while for the case $i = m$ 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 $j = m$ and $i = 1$ in (3.89), so $g_{\mathrm{ev}} = (1 + \gamma_{|\frac{m}{2}+1-i|}/2\alpha_1)(\sqrt{\varepsilon_1}/\alpha_{|\frac{m}{2}+1-i|}) + \sqrt{\varepsilon_1/\alpha_1}/2$. Similarly it can be shown that:

$$
\begin{aligned}
&\left\|\left(B'_i - s'_i B'_{\frac{m}{2},\frac{m}{2}+1} - c'_i B'_{1,-m}\right)|\psi'\rangle\right\| \\
&= \frac{1}{2}\left\|\left(B'_i - B'_{1-i} - \xi_{\frac{m}{2}-i} B'_{\frac{m}{2},\frac{m}{2}+1} + B'_i + B'_{1-i} - \xi_{i-1} B'_{1,-m}\right)|\psi'\rangle\right\| \\
&\leq \frac{1}{2}\left\|\left(B'_i - B'_{1-i} - \xi_{\frac{m}{2}-i} B'_{\frac{m}{2},\frac{m}{2}+1}\right)|\psi'\rangle\right\| + \frac{1}{2}\left\|\left(B'_i + B'_{1-i} - \xi_{i-1} B'_{1,-m}\right)|\psi'\rangle\right\| \\
&\leq \sqrt{\varepsilon_1}\left(\frac{1}{\alpha_{i-1}} + \frac{1}{\tilde{\alpha}_{\frac{m}{2}-i}}\right) = h_{\mathrm{ev}}, \qquad (3.117)
\end{aligned}
$$

where in the last inequality we used already established bounds given in equations (3.96) and (3.97) and we introduced notation $\tilde{\alpha}_{m/2-i}$ which is equal to $\alpha_{m/2-i}$ when $m/2 > i$, and to $\alpha_{i-1-m/2}$ otherwise (for the clarification see the text following equation (3.64)). Similarly to the previous case the bound is properly defined unless $i \in \{1, m, m/2, m/2+1\}$. For the cases $i = 1, m$ the norm $\|(B'_i + B'_{1-i} - \xi_{i-1}B'_{1,-m})|\psi'\rangle\|$ is trivial, thus equal to 0, so we have $h_{\mathrm{ev}} = \sqrt{\varepsilon_1}/\tilde{\alpha}_{m/2-i}$. Similarly when $i = m/2, m/2+1$, the norm $\|(B'_i - B'_{1-i} - \xi_{\frac{m}{2}-i}B'_{\frac{m}{2},\frac{m}{2}+1})|\psi'\rangle\|$ is equal to 0, causing h_{ev} to be equal to

$\sqrt{\varepsilon_1}/\alpha_{i-1}$. By repeating an analogue procedure it is straightforward to obtain bounds for the case when the number of inputs is odd:

$$g_{\text{odd}} = \sqrt{\varepsilon_1}\left(\frac{1}{\tilde{\alpha}_{\frac{m+1}{2}-i}} + \left(1+\frac{\gamma_{i-1}}{2\alpha_1}\right)\frac{1}{\alpha_{i-1}}\right), \tag{3.118}$$

$$h_{\text{odd}} = \sqrt{\varepsilon_1}\left(\frac{1}{\alpha_{i-1}} + \left(1+\frac{\gamma_{|\frac{m+1}{2}-i|}}{2\alpha_1}\right)\frac{1}{\alpha_{|\frac{m+1}{2}-i|}}\right). \tag{3.119}$$

Similarly to the case when the number of inputs is even, for $i=1,m$ the expression for g_{odd} is estimated to be $\sqrt{\varepsilon_1}/\tilde{\alpha}_{\frac{m+1}{2}-i}$ and for $i=(m+1)/2,(m+3)/2$ it reduces to $\left[\sqrt{\varepsilon_1}/\alpha_{i-1}\right](1+\gamma_{i-1}/(2\alpha_1))$. Also, for $i=(m+1)/2$ we have $h_{\text{odd}}=\sqrt{\varepsilon_1}/\alpha_{i-1}$, and for $i=1,m$ we estimate $h_{\text{odd}}=[\sqrt{\varepsilon_1}/\alpha_{|\frac{m+1}{2}-i|}](1+\gamma_{|\frac{m+1}{2}-i|}/(2\alpha_1))$.

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

Finally, in the robust case, we need an extra lemma to take into account the normalisation of the junk state $|\varphi\rangle$.

Lemma 3.10. *Let $|\varphi\rangle$ be the state of the additional degrees of freedom from Theorem 3.6 and $|\varphi'\rangle$ the state defined in (3.131). Then,*

$$\||\varphi\rangle - |\varphi'\rangle\| \leq \left(\frac{1}{2}+\sqrt{2}\right)\sqrt{\varepsilon_1} + \frac{\omega'}{4}, \tag{3.120}$$

where $\omega' \equiv \omega_{\text{ev}}$ for even m and $\omega' \equiv \omega_{\text{odd}}$ for odd m.

Proof. Let us notice that $\||\varphi\rangle - |\varphi'\rangle\| = \||\varphi'\rangle\| - 1$ and then by using the explicit form of $|\varphi'\rangle$ and the inequalities (3.85) and (3.87), we can write

$$\begin{aligned}
\||\varphi'\rangle\| &\leq \frac{1}{2\sqrt{2}}\left(\|(\mathbb{I}+Z'_A)(\mathbb{I}+Z'_B)|\psi'\rangle\| + 2\sqrt{\varepsilon_1}\right) \\
&\leq \frac{1}{2\sqrt{2}}\left[\|(\mathbb{I}+Z'_A)^2|\psi'\rangle\| + 4\sqrt{\varepsilon_1}\right] \\
&= \frac{1}{\sqrt{2}}\|(\mathbb{I}+Z'_A)|\psi'\rangle\| + \sqrt{2\varepsilon_1}.
\end{aligned} \tag{3.121}$$

Now we want to estimate $||\psi'\rangle Z'_A|\psi'\rangle|$. For this we will proceed as in [MYS12]. Note that due to the unitarity of Z'_A and equations (3.85) and (3.86), we can write $\|\,(Z'_AX'_B + X'_AZ'_A)|\psi'\rangle\| \;= \|\,(Z'_AX'_B - Z'_AX'_A + Z'_AX'_A + X'_AZ'_A)|\psi'\rangle\| \;\leq$

$\sqrt{\varepsilon_1} + \omega'$. 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

$$|\langle\psi'|Z'_A|\psi'\rangle + \langle\psi'|X'_B Z'_A X'_A|\psi'\rangle| \leq \sqrt{\varepsilon_1} + \omega'. \tag{3.122}$$

On the other hand, using the unitarity of $\langle\psi'|Z'_A$ and result (3.85), we can write

$$|\langle\psi'|Z'_A|\psi'\rangle - \langle\psi'|X'_B Z'_A X'_A|\psi'\rangle| \leq \sqrt{\varepsilon_1}. \tag{3.123}$$

Finally, if we sum equations (3.122) and (3.123) we get

$$|\langle\psi'|Z'_A|\psi'\rangle| \leq \sqrt{\varepsilon_1} + \omega'/2. \tag{3.124}$$

If we plug this result in (3.121) we will get

$$\begin{aligned} \| \, |\varphi'\rangle\| \quad &\leq \sqrt{\langle\psi'|(\mathbb{I} + Z'_A)|\psi'\rangle} + \sqrt{2\varepsilon_1} \\ &\leq \sqrt{1 + \sqrt{\varepsilon_1} + \omega'/2} + \sqrt{2\varepsilon_1} \\ &\leq 1 + (\tfrac{1}{2} + \sqrt{2})\sqrt{\varepsilon_1} + \tfrac{\omega'}{4} \end{aligned} \tag{3.125}$$

This estimation concludes the proof, since it is straightforward to check that the expression (3.120) is satisfied. □

3.4.2. Robust self-test

Equipped with the results of Section 3.4.1, we can state and prove our second main result. For simplicity and clearness we give bounds for the case when the number of measurements is even; the bounds for in the odd m case can be determined in an analogous way.

Theorem 3.11. *Let $\{|\psi'\rangle, A'_i, B'_i\}$ be a state and measurements giving a violation of the chained Bell inequality of $B_m^{\max} - \varepsilon$. Then,*

$$\|\Phi(A'_i B'_j|\psi'\rangle|00\rangle) - |\varphi\rangle A_i B_j|\phi^+\rangle\| \leq f_{ij}(\varepsilon, m), \tag{3.126}$$

$$\|\Phi(A'_i|\psi'\rangle|00\rangle) - |\varphi\rangle A_i|\phi^+\rangle\| \leq f_{A_i}(\varepsilon, m), \tag{3.127}$$

$$\|\Phi(B'_j|\psi'\rangle|00\rangle) - |\varphi\rangle B_j|\phi^+\rangle\| \leq f_{B_j}(\varepsilon, m), \tag{3.128}$$

$$\|\Phi(|\psi'\rangle|00\rangle) - |\varphi\rangle|\phi^+\rangle\| \leq f(\varepsilon, m), \tag{3.129}$$

where $i, j = 1, \ldots, m$, Φ is the unitary transformation defined in Figure 3.2, $|\varphi\rangle = (1/N)(\mathbb{I} + Z'_A)(\mathbb{I} + \widetilde{Z}'_B)|\psi'\rangle$ with N denoting the length of $|\varphi\rangle$. The functions $f(\varepsilon, m)$, $f_{B_j}(\varepsilon, m)$, $f_{A_i}(\varepsilon, m)$ and $f_{ij}(\varepsilon, m)$ vanish as $\varepsilon \to 0$ and for sufficiently large m scale with m as m^2.

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

$$\|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - |\varphi'\rangle A_iB_j|\phi^+\rangle\| \tag{3.130}$$

with

$$|\varphi'\rangle = \frac{1}{2\sqrt{2}}(\mathbb{I} + Z_A')(\mathbb{I} + \widetilde{Z}_B')|\psi'\rangle. \tag{3.131}$$

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 3.6 replacing the identities by the corresponding inequalities. First, let us notice that for any $i = 1,\ldots,m$ (see 3.4.1 for the proof):

$$\|[A_i' - (s_iX_A' + c_iZ_A')]|\psi'\rangle\| \leq g_{\mathrm{ev}}, \qquad \|[B_i' - (s_i'X_B' + c_i'Z_B')]|\psi'\rangle\| \leq h_{\mathrm{ev}}, \tag{3.132}$$

where g_{ev} and h_{ev} are given in Lemma 3.9 of the Appendix. Denoting by $\overline{A}_i$ and $\overline{B}_i$ the operators appearing in the parentheses in (3.132), we can write

$$\begin{aligned}\|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - |\varphi'\rangle A_iB_j|\phi^+\rangle\| \;\leq\; & \|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - \Phi(\overline{A}_i\overline{B}_j|\psi'\rangle|00\rangle)\| \\ & + \|\Phi(\overline{A}_i\overline{B}_j|\psi'\rangle|00\rangle) - |\varphi'\rangle A_iB_j|\phi^+\rangle\|,\end{aligned} \tag{3.133}$$

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

$$\begin{aligned}\|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - \Phi(\overline{A}_i\overline{B}_j|\psi'\rangle|00\rangle)\| \;&\leq\; \|(A_i'B_j' - \overline{A}_i\overline{B}_j)|\psi'\rangle\| \\ &\leq\; \|(A_i' - \overline{A}_i)|\psi'\rangle\| + \|(B_j' - \overline{B}_j)|\psi'\rangle\| \\ &\leq\; g_{\mathrm{ev}} + h_{\mathrm{ev}},\end{aligned} \tag{3.134}$$

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 (3.134) stems directly from (3.132). In the cases when A_i' or B_j' are equal to the identity operator $\mathbb{I}$, the above bound is replaced by h_{ev} and g_{ev}, respectively, while in the case $A_i' = B_j' = \mathbb{I}$, this distance is simply zero.

Let us then concentrate on the second norm of the right-hand side of (3.133). Exploiting the explicit forms of the operators $\overline{A}_i$ and $\overline{B}_i$ and the measurements

A_i and B_i, one has

$$\begin{aligned}\|\Phi(\overline{A}_i\overline{B}_j|\psi'\rangle|00\rangle)-|\varphi'\rangle A_iB_j|\phi^+\rangle\| \;\leq\; & \|\Phi(X'_AX'_B|\psi'\rangle|00\rangle)-|\varphi'\rangle X_AX_B|\phi^+\rangle\|\\ &+\|\Phi(X'_AZ'_B|\psi'\rangle|00\rangle)-|\varphi'\rangle X_AZ_B|\phi^+\rangle\|\\ &+\|\Phi(Z'_AX'_B|\psi'\rangle|00\rangle)-|\varphi'\rangle Z_AX_B|\phi^+\rangle\|\\ &+\|\Phi(Z'_AZ'_B|\psi'\rangle|00\rangle)-|\varphi'\rangle Z_AZ_B|\phi^+\rangle\|.\end{aligned}\tag{3.135}$$

Let us consider the first and the last norm on the right-hand side of this inequality. With the aid of inequalities (3.85) and the fact that $X_AX_B|\phi^+\rangle = Z_AZ_B|\phi^+\rangle = |\phi^+\rangle$, both can be upper bounded by $\sqrt{\varepsilon_1}+\|\Phi(|\psi'\rangle|00\rangle)-|\varphi'\rangle|\phi^+\rangle\|$. Then, from the definition of the unitary operation Φ and the state $|\varphi'\rangle$ it follows that the latter norm can be upper bounded as

$$\begin{aligned}\|\Phi(|\psi'\rangle|00\rangle)-|\varphi'\rangle|\phi^+\rangle\| \;\leq\; & \frac{1}{4}\Big(\|X_A(\mathbb{I}-Z_A)(\mathbb{I}+\widetilde{Z}_B)|\psi'\rangle\|\\ &+\|\widetilde{X}_B(\mathbb{I}+Z_A)(\mathbb{I}-\widetilde{Z}_B)|\psi'\rangle\|\\ &+\|X_A\widetilde{X}_B(\mathbb{I}-Z_A)(\mathbb{I}-\widetilde{Z}_B)|\psi'\rangle-|\varphi'\rangle\|\Big).\end{aligned}\tag{3.136}$$

To upper bound the first two norms in (3.136), we first exploit inequalities (3.85) and (3.87) 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 $(\mathbb{I}+Z'_A)(\mathbb{I}-Z'_A)=0$. To upper bound the last norm in (3.136), we first use the anticommutation relation (3.86) which leads us to

$$\begin{aligned}&\|X_A\widetilde{X}_B(\mathbb{I}-Z_A)(\mathbb{I}-\widetilde{Z}_B)|\psi'\rangle-|\varphi'\rangle\|\\ &\leq 2\omega_{\mathrm{ev}}(m)+2\|X_A\widetilde{X}_B(\mathbb{I}-\widetilde{Z}_B)|\psi'\rangle-(\mathbb{I}+\widetilde{Z}_B)|\psi'\rangle\|.\end{aligned}\tag{3.137}$$

One then uses again inequalities (3.85) and (3.87) in order to "convert" $\widetilde{Z}_B$ to Z_B and then Z_B to Z_A. This gives

$$\begin{aligned}&\|X_A\widetilde{X}_B(\mathbb{I}-Z_A)(\mathbb{I}-\widetilde{Z}_B)|\psi'\rangle-|\varphi'\rangle\|\\ &\leq 2\omega_{\mathrm{ev}}(m)+8\sqrt{\varepsilon_1}+2\|X_A\widetilde{X}_B(\mathbb{I}-Z_A)|\psi'\rangle-(\mathbb{I}+Z_A)|\psi'\rangle\|.\end{aligned}\tag{3.138}$$

After applying (3.86) and then (3.85) and (3.87), one finally arrives at

$$\|X_A\widetilde{X}_B(\mathbb{I}-Z_A)(\mathbb{I}-\widetilde{Z}_B)|\psi'\rangle-|\varphi'\rangle\|\leq 4\omega_{\mathrm{ev}}(m)+16\sqrt{\varepsilon_1}.\tag{3.139}$$

Taking all this into account, we have that

$$\|\Phi(|\psi'\rangle|00\rangle)-|\varphi'\rangle|\phi^+\rangle\|\leq 6\sqrt{\varepsilon_1}+\omega_{\mathrm{ev}}(m).\tag{3.140}$$

Let us now pass to the second norm in (3.135) and notice that by using inequality (3.85) and the fact that $Z_B|\phi^+\rangle = Z_A|\phi^+\rangle$, it can be upper bounded in the following way

$$\begin{aligned}
&\|\Phi(X'_A Z'_B|\psi'\rangle|00\rangle) - |\varphi'\rangle X_A Z_B|\phi^+\rangle\| \\
&\leq \sqrt{\varepsilon_1} + \frac{1}{4}\Big(\|(\mathbb{I}+Z'_A)(\mathbb{I}+\widetilde{Z}_B)X'_A Z'_A|\psi'\rangle\| \\
&\qquad\qquad + \|X'_A\widetilde{X}_B(\mathbb{I}+Z'_A)(\mathbb{I}+\widetilde{Z}_B)X'_A Z'_A|\psi'\rangle\| \\
&\qquad\qquad + \|X'_A(\mathbb{I}-Z'_A)(\mathbb{I}+\widetilde{Z}_B)X'_A Z'_A|\psi'\rangle - |\varphi'\rangle\| \\
&\qquad\qquad + \|\widetilde{X}_B(\mathbb{I}+Z'_A)(\mathbb{I}-\widetilde{Z}_B)X'_A Z'_A|\psi'\rangle + |\varphi'\rangle\|\Big). \qquad (3.141)
\end{aligned}$$

Let us consider the first two norms appearing on the right-hand side of (3.141). Exploiting the anticommutation relation (3.86) and then inequalities (3.85) and (3.87) to convert $\widetilde{Z}_B$ to Z_A, we can bound each of these norms by $4\sqrt{\varepsilon_1} + 2\omega_{\mathrm{ev}}(m)$. Using then the inequality (3.86), the third term is not larger than $2\omega_{\mathrm{ev}}(m)$. To bound the fourth term in (3.141), let us use the fact that $\|\mathbb{I} + Z'_A\| \leq 2$ to write

$$\begin{aligned}
&\|\widetilde{X}_B(\mathbb{I}+Z'_A)(\mathbb{I}-\widetilde{Z}_B)X'_A Z'_A|\psi'\rangle - |\varphi'\rangle\| \\
&\leq 2\|\widetilde{X}_B(\mathbb{I}-\widetilde{Z}_B)X'_A Z'_A|\psi'\rangle - (\mathbb{I}+\widetilde{Z}_B)|\psi'\rangle\|. \qquad (3.142)
\end{aligned}$$

Subsequent use of inequalities (3.85) and (3.87) to $\widetilde{Z}_B$ and $\widetilde{X}_B$ gives

$$\begin{aligned}
&\|\widetilde{X}_B(\mathbb{I}+Z'_A)(\mathbb{I}-\widetilde{Z}_B)X'_A Z'_A|\psi'\rangle - |\varphi'\rangle\| \\
&\leq 16\sqrt{\varepsilon_1} + 2\|X'_A Z'_A(\mathbb{I}-Z'_A)X'_A|\psi'\rangle - (\mathbb{I}+Z'_A)|\psi'\rangle\|, \qquad (3.143)
\end{aligned}$$

which after a double application of (3.86) yields

$$\|\widetilde{X}_B(\mathbb{I}+Z'_A)(\mathbb{I}-\widetilde{Z}_B)X'_A Z'_A|\psi'\rangle - |\varphi'\rangle\| \leq 16\sqrt{\varepsilon_1} + 2\omega_{\mathrm{ev}}(m). \qquad (3.144)$$

This together with previous estimations finally implies that

$$\|\Phi(X'_A Z'_A|\psi'\rangle|00\rangle) - |\varphi'\rangle X_A Z_B|\phi^+\rangle\| \leq 7\sqrt{\varepsilon_1} + 2\omega_{\mathrm{ev}}(m). \qquad (3.145)$$

In a fully analogous way one can estimate the third term on the right-hand side of (3.135)

$$\|\Phi(Z'_A X'_B|\psi'\rangle|00\rangle) - |\varphi'\rangle Z_A X_B|\phi^+\rangle\| \leq 7\sqrt{\varepsilon_1} + 2\omega_{\mathrm{ev}}(m). \qquad (3.146)$$

By plugging all these terms into (3.135) and then the resulting inequality together with (3.134) into (3.133), one obtains

$$\|\Phi(A'_i B'_j|\psi'\rangle|00\rangle) - |\varphi'\rangle A_i B_j|\phi^+\rangle\| \leq 28\sqrt{\epsilon_1} + 6\omega_{\mathrm{ev}}(m) + g_{\mathrm{ev}} + h_{\mathrm{ev}}. \qquad (3.147)$$

The terms from (3.127) can be treated in almost exactly the same way, giving

$$\|\Phi(A_i'|\psi'\rangle|00\rangle) - |\varphi'\rangle A_i|\phi^+\rangle\| \leq 12\sqrt{\varepsilon_1} + 3\omega_{\text{ev}}(m) + g_{\text{ev}}, \tag{3.148}$$

while the estimation of the corresponding expression from (3.127) follows from the application of inequality (3.85) to (3.148), meaning that an additional error of $\sqrt{\varepsilon_1}$ has to be taken into account, which gives

$$\|\Phi(B_j'|\psi'\rangle|00\rangle) - |\varphi'\rangle B_j|\phi^+\rangle\| \leq 13\sqrt{\varepsilon_1} + 3\omega_{\text{ev}}(m) + h_{\text{ev}}. \tag{3.149}$$

Finally, the case of $A_i' = B_j' = \mathbb{I}$ has already been derived in (3.140).

The distance between the normalized state $|\varphi\rangle$ and the unnormalized one $|\varphi'\rangle$ is estimated in Lemma 3.10 to be

$$\||\varphi\rangle - |\varphi'\rangle\| \leq \left(\frac{1}{2} + \sqrt{2}\right)\sqrt{\varepsilon_1} + \omega', \tag{3.150}$$

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

In order to obtain inequalities (3.126) and complete the proof we use the triangle inequality for the vector norm to write

$$\begin{aligned}\|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - |\varphi\rangle A_iB_j|\phi^+\rangle\| \quad &\leq \quad \|\Phi(A_i'B_j'|\psi'\rangle|00\rangle) - |\varphi'\rangle A_iB_j|\phi^+\rangle\| \\ &\quad + \||\varphi\rangle - |\varphi'\rangle\|, \end{aligned} \tag{3.151}$$

and then apply the previously determined inequalities (3.140), (3.147), (3.148), (3.149) and (3.150). All terms contributing to the functions $f(\varepsilon, m)$, $f_{B_j}(\varepsilon, m)$, $f_{A_i}(\varepsilon, m)$ and $f_{ij}(\varepsilon, m)$ scale at most as $O(m^2\sqrt{\epsilon})$. The more detailed analysis of the asymptotic behaviour of different contributions is discussed in Lemmas 3.8 and 3.9. □

Let us remark here that we have not checked whether the bounds (3.126)–(3.129) are optimal both in the distance from the maximal quantum violation ε and the number of measurements m. Thus, it is still possible that these robustness bounds scale better than quadratically with the number of measurements. However, in order to determine such tighter bounds one would need in particular to optimise the above method over all SOS decompositions, which is certainly a difficult task.

3.5. Applications: randomness

It was shown in [DPA13] that by exploiting the symmetries of the chained Bell inequalities, two bits of global randomness can be certified when the maximum quantum violation of these inequalities is achieved, provided this maximal quantum violation is unique. This latter assumption had not been proven – with our results, we confirm that the maximal quantum violation is indeed unique and we complete the proof of [DPA13].

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

$$\hat{I}^m_{\mathrm{ch}} := I^m_{\mathrm{ch}} + \langle A_1 B_{m+1}\rangle \leq 2m - 1 \tag{3.152}$$

in which Alice, as before, can measure one of m observables A_i while Bob has $m+1$ observables B_i at his disposal, where m is assumed to be even. It is not difficult to see that the maximal quantum violation of this inequality amounts to $\hat{B}^{\max}_m = B^{\max}_m + 1$.

Let us now assume that $|\psi'\rangle$ and A'_i and B'_i are the state and the measurements maximally violating (3.152). Denoting then by $\hat{\mathcal{B}}_m = \mathcal{B}_m + A'_1 \otimes B'_{m+1}$ the corresponding Bell operator, one has $\langle\psi|(\hat{B}^{\max}_m \mathbb{I} - \hat{\mathcal{B}}_m)|\psi\rangle = 0$, which, owing to the fact that $|\psi\rangle$ also violates maximally the chained Bell inequality and that $B^{\max}_m$ is its maximal quantum violation, simplifies to $0 = \langle\psi|(\mathbb{I} - A'_1 \otimes B'_{m+1})|\psi\rangle = (1/2)\langle\psi|(\mathbb{I} - A'_1 \otimes B'_{m+1})^2|\psi\rangle$, where the second equality is a consequence of the fact that A'_1 and B'_{m+1} are unitary and hermitian. This implies that

$$A'_1|\psi\rangle = B'_{m+1}|\psi\rangle. \tag{3.153}$$

This property implies in particular that $\langle B'_{m+1}\rangle = \langle A'_1\rangle$, which, taking into account the fact that for the maximal quantum violation of the chained Bell inequality $\langle A'_i\rangle = 0$ for any $i = 1, \ldots, m$, implies $\langle B'_{m+1}\rangle = 0$. In a quite analogous way we can now prove that the expectation value $\langle A'_{m/2+1} B'_{m+1}\rangle = \langle\psi|A'_{m/2+1} \otimes B'_{m+1}|\psi\rangle$ vanishes. Exploiting (3.153), we can rewrite it as $\langle\psi|A'_{m/2+1} \otimes B'_{m+1}|\psi\rangle = \langle\psi|A'_{m/2+1}A'_1|\psi\rangle$. Then, due to the fact that the expectation value $\langle\psi|A'_{m/2+1} \otimes B'_{m+1}|\psi\rangle$ is real and both operators $A'_{m/2+1}$ and B'_{m+1} are hermitian, which means that $\langle\psi|A'_{m/2+1}A'_1|\psi\rangle = \langle\psi|A'_1 A'_{m/2+1}|\psi\rangle$, this can be further rewritten as

$$\langle A'_{m/2+1} B'_{m+1}\rangle = \frac{1}{2}\langle\psi|\{A'_1, A'_{\frac{m}{2}+1}\}|\psi\rangle. \tag{3.154}$$

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

$$P(a, b|x = \frac{m}{2} + 1, y = m + 1) = \frac{1}{4} \tag{3.155}$$

with $a, b = 0, 1$. All this proves that any probability distribution $P(a, b|i, j)$ with $i = 1, \ldots, m$ and $j = 1, \ldots, m + 1$ maximally violating the modified chained Bell inequality (3.152) is such that all outcomes of the pair of measurements $A'_{m/2+1}, B'_{m+1}$ are equiprobable (3.155) and thus perfectly random, meaning that (3.152) certifies two bits of perfect randomness.

The intuition behind the above approach is very simple. At the maximal quantum violation of (3.152) the measurement B'_{m+1} must be "parallel" to A'_1 (see (3.153)). Therefore it is "orthogonal" to $A'_{m/2+1}$ as the latter is orthogonal to A'_1, meaning that $\langle A'_{m/2+1} B'_{m+1} \rangle = 0$ which is basically what we need. It is worth noticing that in the even m case all pairs $A'_{1+i}, A'_{m/2+i}$ with $i = 1, \ldots, m/2 - 1$ of Alice's observables are orthogonal, and therefore our argument can be extended to any pair $A'_{m/2+i}, B'_{m+1}$, that is, $\langle A'_{m/2+i}, B'_{m+1} \rangle = 0$ provided the Bell inequality $I^m_{\text{ch}} + \langle A_{m/2+i} B_{m+1} \rangle \leq 2m - 1$ is maximally violated. Unfortunately, this approach does not work in the odd m case as no pair of observables at Alice's or Bob's sides are orthogonal.

3.6. Discussion

We developed a scheme for self-testing the maximally entangled state of two qubits using the chained Bell inequalities. Our results hold for any number of inputs, which allows for the self-test of measurements on the whole XZ plane of the Bloch sphere – this is particularly interesting since self-testing of measurements has not been studied extensively. Some of the previous self-testing techniques found an application for blind quantum computation protocols (see [RUV13, BFK09]). The fact that the chained Bell inequalities involve and certify a quite 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 [DPA13], this property was assumed to be true to argue maximal randomness certification in Bell tests: with our proof, their results are now confirmed.

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? We partially address this question in Chapter 4, where we construct Bell inequalities for any number of inputs and outputs that reduce to the chained Bell inequalities when the number of outputs is set to two.

4. Bell inequalities tailored to maximally entangled states

In this chapter, we introduce Bell inequalities valid for an arbitrary number of measurements and outcomes, whose maximal quantum violation is attained by the maximally entangled states

$$|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle. \tag{4.1}$$

Quantum theory is a key ingredient in how we construct these Bell inequalities, which is the main novelty of our approach. Indeed, since Bell inequalities were first developed to detect nonlocality, the standard approach for their construction was to derive constraints satisfied by local models – i.e. using techniques in convex geometry, as the local set is a polytope. In our method on the other hand, we start from quantum theory and exploit the symmetries and perfect correlations of maximally entangled states, as well as SOS decompositions of Bell operators.

Very importantly, we are able to compute analytically the quantum, classical and no-signalling bounds of our Bell expressions. We also discuss their applications to device-independent protocols. Maximal violation by the maximally entangled state is a desirable property, since these states have particular features such as perfect correlations between outcomes of local measurements in the same bases, and therefore many quantum information protocols rely on them.

We start with our main results, which concern the bipartite case. We detail the method that leads to our Bell expressions and we study their properties. We then present an extension of our results to the multipartite case, where the optimal states are now the generalised GHZ states (2.4). We also discuss a modification of our Bell expressions for the case of three outcomes, which leads to a class of Bell inequalities suited to partially entangled states. Finally, we present the results of an experimental collaboration in which we participated.

4.1. The bipartite case

As we just mentioned, Bell inequalities were at first developed to detect nonlocality, and they have been constructed accordingly. Facet (or tight) Bell inequalities such as the CHSH inequalities [CHSH69] and the Collins-Gisin-Linden-Massar-Popescu (CGLMP) inequalities [CGL$^+$02] provide necessary and sufficient criteria to detect the nonlocality of given correlations. In the DI setting however, Bell inequalities have acquired a new role as certificates of quantum properties. The existing Bell inequalities, built with nonlocality detection as a goal, are not necessarily optimal for inferring specific quantum properties in the DI setting. For instance, in a scenario where two binary measurements are performed on two entangled subsystems, certain "non-facet" Bell inequalities are better certificates of randomness than CHSH when the two quantum systems are partially entangled [AMP12].

In the case where only two measurements are made on each subsystem, all facet Bell inequalities are known for a small number of outputs and they are of the CGLMP form [CGL$^+$02]. However, they are not maximally violated by the maximally entangled states of two qudits, except in the case of two measurement outcomes corresponding to the CHSH inequality – this was at first considered an "anomaly" in the relation between nonlocality and entanglement [ADGL02, ZG08]. For instance, in the case of three outcomes, the state maximally violating the CGLMP inequality is $|\psi_\gamma\rangle = (|00\rangle + |11\rangle + |22\rangle)/(\sqrt{2+\gamma^2})$ with $\gamma = (\sqrt{11} - \sqrt{3})/2$.

Our aim is to introduce a family of Bell expressions, whose maximal quantum value is attained by the *two-qudit* maximally entangled state $|\phi_d^+\rangle$, in a general Bell scenario of m inputs and d outputs. In the particular case of two measurements, CHSH is the simplest example of a Bell inequality with this property, but others are known [SLK06, LCL07, dV15] (see also results for many settings [JLL$^+$08, LLD09, LRY$^+$10]). Our construction works, however, for arbitrary numbers of measurements and outcomes, and, crucially, all three quantum, classical, and no-signalling bounds can be computed analytically as functions of m and d. Since we are not using local constraints in our construction we should not expect our Bell inequalities to be tight, and indeed they are not.

4.1.1. Class of Bell expressions

We start our construction from the premise that the maximal quantum values of the Bell expressions we wish to derive are obtained when Alice and Bob perform what we call the optimal CGLMP measurements. The resulting probabilities possess symmetries, which we exploit.

Optimal measurements and symmetries

The measurements that we call optimal CGLMP measurements were first introduced in [KGZ+00] and generalised to an arbitrary number of inputs in [BKP06], where a many-input generalisation of the CGLMP inequalities was introduced, called the Barrett-Kent-Pironio (BKP) inequalities. This choice of optimal measurements stems from the fact that they generalise the ideal CHSH measurements ($d = 2$) to arbitrary dimensions. They also lead to non-local correlations that are most robust to noise [KGZ+00] or that give a stronger statistical test for $m = 2$ [AGG05]. The eigenvectors characterising Alice's measurement x are given by

$$|a_x\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \exp\Big(\frac{2\pi i}{d} q(a - \theta_x)\Big) |q\rangle, \tag{4.2}$$

and those characterising Bob's measurement y are given by

$$|b_y\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \exp\Big(-\frac{2\pi i}{d} q(b - \zeta_y)\Big) |q\rangle, \tag{4.3}$$

with the phases $\theta_x = (x - 1/2)/m$ and $\zeta_y = y/m$ for $x, y = 1, \ldots, m$. They can be understood as applying a variable phase and performing a Fourier transform. When applying the optimal CGLMP measurements on a normalised state of the form $|\psi\rangle = \sum_{q=0}^{d-1} \gamma_q |qq\rangle$, we obtain the probabilities

$$P(a, b|x, y) = \left| \frac{1}{d} \sum_{q=0}^{d-1} \gamma_q \exp\left(\frac{2\pi i}{d} q(a - b - \theta_x + \zeta_y)\right) \right|^2 . \tag{4.4}$$

Let us study the symmetries of these probabilities. One can observe that expression (4.4) depends only on the difference $a - b = k \bmod d$ and not on a and b separately. Defining:

$$P(A_x = B_y + k) = \sum_{j=0}^{d-1} P(j + k \bmod d, j|x, y), \tag{4.5}$$

where the addition is modulo d, this first symmetry means that

$$P(A_x = B_y + k) = dP(k, 0|x, y). \tag{4.6}$$

That is, all the terms $P(A_x = B_y + k)$ computed for those measurements and state have identical subterms $P(j + k \bmod d, j|x, y)$. If we impose that our

Bell expressions respect this symmetry, the probabilities $P(j+k \bmod d, j|x,y)$ should be treated equally for all j, i.e., the Bell expressions should be linear combinations of $P(A_x = B_y + k)$. Moreover, using the values of the phases θ_x and ζ_y, one can verify straightforwardly that expression (4.4) has the same value if $x = y$ and $a - b = k$, and if $x = y + 1$ and $a - b = -k$. Thus :

$$P(A_i = B_i + k) = P(B_i = A_{i+1} + k), \tag{4.7}$$

for $i = 1, \ldots, m$. Note that if one wishes to write $A_{m+1} = A_1$, the symmetry is not valid anymore and requires the definition $A_{m+1} = A_1 + 1$, which we impose. Taking into account all symmetries, a generic form for our Bell expressions is

$$I_{m,d} = \sum_{k=0}^{\lfloor d/2 \rfloor - 1} \left(\alpha_k \mathbb{P}_k - \beta_k \mathbb{Q}_k \right), \tag{4.8}$$

where

$$\begin{aligned} \mathbb{P}_k &= \sum_{i=1}^{m} [P(A_i = B_i + k) + P(B_i = A_{i+1} + k)], \\ \mathbb{Q}_k &= \sum_{i=1}^{m} [P(A_i = B_i - k - 1) + P(B_i = A_{i+1} - k - 1)], \end{aligned} \tag{4.9}$$

with $A_{m+1} = A_1 + 1$. To sum up, all terms who have the same value when evaluated as (4.4) appear with the same coefficient α_k or β_k in the Bell expression, thus forming "blocks" $\mathbb{P}_k$ and $\mathbb{Q}_k$. Different blocks have different values and are multiplied by different coefficients: the parameters α_k and β_k are our degrees of freedom. If we take e.g., $\alpha_k = \beta_k = 1 - 2k/(d-1)$ for $m = 2$, we recover the CGLMP Bell inequalities.

Generalised correlators

To exploit the symmetries inherent in Bell inequalities, we often write them in terms of correlators instead of probabilities. As we consider an arbitrary number of outcomes, we appeal to the notion of generalised correlators (see, for instance, [LLD09] and [BBB+12] for other options). These are complex numbers that are defined through the two-dimensional Fourier transform of the probabilities $P(a,b|x,y)$:

$$\langle A_x^k B_y^l \rangle = \sum_{a,b=0}^{d-1} \omega^{ak+bl} P(a,b|x,y), \tag{4.10}$$

where $\omega = \exp(2\pi i/d)$, $k, l \in \{0, \ldots, d-1\}$, and $\{A_x^k\}_k$ and $\{B_y^l\}_l$ can be thought of as generalised observables, or measurements with outcomes labelled by roots of unity ω^j $(j = 0, \ldots, d-1)$. For quantum correlations $\vec{p}$, the correlators $\langle A_x^k B_y^l \rangle$ are average values of the tensor product of the operators

$$A_x^k = \sum_{a=0}^{d-1} \omega^{ak} M_{a|x} \quad \text{and} \quad B_y^l = \sum_{b=0}^{d-1} \omega^{bl} N_{b|y} \tag{4.11}$$

on the state $|\psi\rangle$. These operators are unitary, their eigenvalues are the roots of unity, and they satisfy $(A_x^k)^\dagger = A_x^{d-k}$ and $(B_y^l)^\dagger = B_y^{d-l}$ for any k, l. The inverse transformation gives:

$$P(a, b|x, y) = \frac{1}{d^2} \sum_{k,l=0}^{d-1} \omega^{-(ak+bl)} \langle A_x^k B_y^l \rangle. \tag{4.12}$$

For the $P(A_x = B_y + k)$, we have:

$$P(A_x = B_y + k) = \frac{1}{d} \sum_{l=0}^{d-1} \omega^{-kl} \langle A_x^l B_y^{d-l} \rangle. \tag{4.13}$$

Using these generalised observables, the optimal CGLMP measurements can be written as:

$$A_x = U_x^\dagger F \Omega F^\dagger U_x, \qquad B_y = V_y F^\dagger \Omega F V_y^\dagger, \tag{4.14}$$

where $\Omega = \text{diag}[1, \omega, \omega^2, \ldots, \omega^{d-1}]$, with $\omega = \exp(2\pi i/d)$, and F is the $d \times d$ discrete Fourier transform matrix given by

$$F_d = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{ij} |i\rangle\langle j|. \tag{4.15}$$

Then, U_x and V_x are unitary operations defining Alice's and Bob's measurements and read explicitly

$$U_x = \sum_{j=0}^{d-1} \omega^{j\theta_x} |j\rangle\langle j|, \qquad V_y = \sum_{j=0}^{d-1} \omega^{j\zeta_y} |j\rangle\langle j|, \tag{4.16}$$

with the same phases as above: $\theta_x = (x - 1/2)/m$ and $\zeta_y = y/m$ for $x, y = 1, \ldots, m$.

Now, exploiting these definitions, in particular equation (4.13), we can rewrite Bell expression (4.8) as

$$\widetilde{I}_{m,d} = \sum_{i=1}^{m}\sum_{l=1}^{d-1}\langle A_i^l \bar{B}_i^l\rangle, \tag{4.17}$$

where, for clarity, the change of variables

$$\bar{B}_i^l = a_l B_i^{d-l} + a_l^* B_{i-1}^{d-l}, \tag{4.18}$$

with $a_l = \sum_{k=0}^{\lfloor d/2\rfloor -1}(\alpha_k \omega^{-kl} - \beta_k \omega^{(k+1)l})$ was introduced on Bob's side. Due to the convention $A_{m+1} = A_1 + 1$, the term $\bar{B}_1^l$ is defined as $\bar{B}_1^l = a_l B_1^{d-l} + a_l^* \omega^l B_m^{d-l}$. For simplicity, in (4.17) we ignored the irrelevant scalar term corresponding to $l = 0$ and rescaled the expression by a factor d. Below we denote the classical, quantum and no-signalling bound of $\widetilde{I}_{m,d}$ by $\widetilde{\beta}_C$, $\widetilde{\beta}_Q$ and $\widetilde{\beta}_{NS}$, respectively, and those of $I_{m,d}$ without the tilde.

Derivation of coefficients α_k and β_k

Our aim now is to fix the free parameters α_k and β_k according to the quantum property we need: maximal violation by the maximally entangled state $|\phi_d^+\rangle$. At this point, it is instructive to look at the specific example of the CHSH Bell expression, as we will want our general expression to reduce to CHSH when $m = 2$, $d = 2$. In the notation (4.17) the CHSH Bell expression $\langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle$ reads

$$\widetilde{I}_{2,2} = \langle A_1 \bar{B}_1\rangle + \langle A_2 \bar{B}_2\rangle, \tag{4.19}$$

where $\bar{B}_1 = (B_1 + B_2)/\sqrt{2}$, $\bar{B}_2 = (B_1 - B_2)/\sqrt{2}$. Then, for the optimal measurements leading to the Tsirelson bound of $\widetilde{I}_{2,2}$, we have $\bar{B}_1 = A_1^*$ and $\bar{B}_2 = A_2^*$. This reflects the property that for the maximally entangled state

$$A \otimes B|\phi_d^+\rangle = \mathbb{1} \otimes AB^T|\phi_d^+\rangle, \quad \forall A, B. \tag{4.20}$$

This condition implies that a measurement by Alice is perfectly correlated with its complex conjugate by Bob. Our intuition to derive Bell inequalities detecting maximal entanglement is to impose this property for any m and d: we choose the parameters α_k and β_k such that conditions

$$\bar{B}_i^l = (A_i^l)^* \tag{4.21}$$

hold for $l = 1, \ldots, d-1$ and $i = 1, \ldots, m$ with the initial operators $\{M_{a|x}\}$ and $\{N_{b|y}\}$ being the optimal CGLMP operators. Conditions (4.21) give rise to a set of linear equations for α_k and β_k which yields

$$\alpha_k = \frac{1}{2d}\tan\left(\frac{\pi}{2m}\right)\left[g(k) - g\left(\left\lfloor\frac{d}{2}\right\rfloor\right)\right], \tag{4.22}$$

$$\beta_k = \frac{1}{2d}\tan\left(\frac{\pi}{2m}\right)\left[g\left(k+1-\frac{1}{m}\right) + g\left(\left\lfloor\frac{d}{2}\right\rfloor\right)\right] \tag{4.23}$$

with $g(x) = \cot(\pi(x+1/2m)/d)$. Let us go over the derivation of these coefficients (4.22) and (4.23) in detail. First, note that the amount of conditions (4.21) can be reduced, as those that hold for $l = 1,\ldots,\lfloor d/2\rfloor$ are the same as those that hold for $l = \lfloor d/2\rfloor + 1,\ldots,d-1$. Indeed,

$$A_x^{d-l} = (A_x^l)^\dagger, \tag{4.24}$$
$$\bar{B}_y^{d-l} = (\bar{B}_y^l)^\dagger. \tag{4.25}$$

Recall that the barred quantities $\bar{B}_i^l$ are defined as

$$\bar{B}_i^l = a_l B_i^{d-l} + a_l^* B_{i-1}^{d-l} \tag{4.26}$$

for $i = 2,\ldots,m$ and $\bar{B}_1^l = a_l B_1^{d-l} + a_l^*\omega^l B_m^{d-l}$, and the numbers a_l are given by

$$a_l = \sum_{k=0}^{\lfloor d/2\rfloor-1}\left[\alpha_k\omega^{-kl} - \beta_k\omega^{(k+1)l}\right]. \tag{4.27}$$

Notice that $a_l = a_{d-l}^*$. Let us notice in passing that the properties (4.24) and (4.25) imply that the Bell expression we consider, i.e.,

$$\widetilde{I}_{m,d} = \sum_{i=1}^{m}\sum_{l=1}^{d-1}\langle A_i^l \bar{B}_i^l\rangle \tag{4.28}$$

is real. This is because the sum in (4.28) can be split into two sums: for $l = 1,\ldots,\lfloor d/2\rfloor$ and $l = \lfloor d/2\rfloor+1,\ldots,d-1$ for odd d, and for $l = 1,\ldots,d/2-1$ and $l = d/2+1,\ldots,d-1$ (plus a single term corresponding to $l = d/2$ which is always real) for even d. Now, due to equations (4.24) and (4.25) one realises that all terms in the second sum are complex conjugations of those in the first sum.

In order to solve the system (4.21) one has to find explicit forms of A_x^l and B_y^l for the CGLMP measurements. Introducing equations (4.15) and (4.16) into (4.14), one obtains

$$A_x^l = \omega^{-(d-l)\theta_x}\sum_{n=0}^{l-1}|d-l+n\rangle\langle n| + \omega^{l\theta_x}\sum_{n=l}^{d-1}|n-l\rangle\langle n| \tag{4.29}$$

and

$$B_y^l = \omega^{-(d-l)\zeta_y} \sum_{n=0}^{l-1} |n\rangle\langle d-l+n| + \omega^{l\zeta_y} \sum_{n=l}^{d-1} |n\rangle\langle n-l|. \tag{4.30}$$

Then, one combines these formulas with equations (4.26) and (4.21), and compares the matrix elements, which yields the following system of equations

$$\begin{array}{rcl} a_l\omega^{-l\zeta_i} + a_l^*\omega^{-l\zeta_{i-1}} & = & \omega^{-l\theta_i} \\ a_l\omega^{(d-l)\zeta_i} + a_l^*\omega^{(d-l)\zeta_{i-1}} & = & \omega^{(d-l)\theta_i}, \end{array} \tag{4.31}$$

with $i = 1, \ldots, m$ and $l = 1, \ldots, \lfloor d/2 \rfloor$, where it is assumed that $\zeta_0 = 0$. Simple algebra implies finally that

$$a_l = \frac{\omega^{\frac{2l-d}{4m}}}{2\cos(\pi/2m)} \qquad (l = 1, \ldots, \lfloor d/2 \rfloor). \tag{4.32}$$

Having determined a_l, one can turn to the system (4.27). It consists of $\lfloor d/2 \rfloor$ equations containing $2\lfloor d/2 \rfloor$ variables, meaning that it cannot be uniquely solved, and, in particular, the solutions will be generally complex. To handle the latter problem we use complex conjugation to equip system (4.27) with $\lfloor d/2 \rfloor$ additional equations

$$\sum_{k=0}^{\lfloor d/2 \rfloor - 1} \left[\alpha_k\omega^{kl} - \beta_k\omega^{-(k+1)l}\right] = a_l^*. \tag{4.33}$$

for $l = 1, \ldots, \lfloor d/2 \rfloor$. Now, both systems (4.27) and (4.33) can be condensed into the following single one

$$\sum_{k=0}^{\lfloor d/2 \rfloor - 1} \left[\alpha_k\omega^{-kl} - \beta_k\omega^{(k+1)l}\right] = c_l, \tag{4.34}$$

in which $c_l = a_l$ for $l = 1, \ldots, \lfloor d/2 \rfloor$ and $c_l = c_{-l}^*$ for $l = -\lfloor d/2 \rfloor, \ldots, -1$. In what follows we solve (4.34) for even and odd d separately.

Odd d**.** We begin by noting that in this case, the system (4.34) consists of $d-1$ equations and involves the same number of variables, and therefore one expects it to have a unique solution. To find it, we denote the set $J := \{-(d-1)/2, \ldots, -1, 1, \ldots, (d-1)/2\}$ and note that for any pair $k, n \in \{0, \ldots, \lfloor d/2 \rfloor - 1\}$, the following identity holds:

$$\sum_{l \in J} \omega^{-lk}\omega^{ln} = \sum_{l \in J \cup \{0\}} \omega^{-lk}\omega^{ln} - 1 = d\delta_{n,k} - 1. \tag{4.35}$$

We then multiply (4.34) by ω^{nl} for some $n \in \{0, \ldots, \lfloor d/2 \rfloor - 1\}$ and add the resulting equations over $l \in J$, which by virtue of equation (4.35) gives

$$\alpha_n = \frac{1}{d} S + \frac{1}{d} \sum_{l \in J} c_l \omega^{nl} \qquad (n = 0, \ldots, \lfloor d/2 \rfloor - 1), \tag{4.36}$$

where we have denoted

$$S = \sum_{k=0}^{\lfloor d/2 \rfloor - 1} (\alpha_k - \beta_k). \tag{4.37}$$

The coefficients β_n can be determined in an analogous way and we obtain:

$$\beta_n = -\frac{1}{d} S - \frac{1}{d} \sum_{l \in J} c_l \omega^{-(n+1)l} \qquad (n = 0, \ldots, \lfloor d/2 \rfloor - 1). \tag{4.38}$$

To fully determine α_n and β_n, it is in fact enough to compute the sum in equation (4.36) as the second one and S can be obtained from it by replacing n by $-(n+1)$ and $\lfloor d/2 \rfloor$, respectively. To compute this sum, we first express it as

$$\begin{aligned} \sum_{l \in J} c_l \omega^{nl} &= \frac{1}{\cos(\pi/2m)} \sum_{l=1}^{\lfloor d/2 \rfloor} \mathrm{Re}\left(\omega^{(2l-d)/4m} \omega^{nl}\right) \\ &= \frac{1}{\cos(\pi/2m)} \left[\cos\left(\frac{\pi}{2m}\right) \sum_{l=1}^{\lfloor d/2 \rfloor} \cos\left(\frac{2\pi l}{d} \xi\right) + \sin\left(\frac{\pi}{2m}\right) \sum_{l=1}^{\lfloor d/2 \rfloor} \sin\left(\frac{2\pi l}{d} \xi\right) \right] \end{aligned} \tag{4.39}$$

where we have denoted $\xi = n + 1/2m$. Using the Euler representations of the cosine and sine functions the above two sums can be computed and they read

$$\sum_{l=1}^{\lfloor d/2 \rfloor} \cos\left(\frac{2\pi l}{d} \xi\right) = \frac{1}{2} \left[\frac{\sin(\pi \xi)}{\sin(\pi \xi / d)} - 1 \right] \tag{4.40}$$

and

$$\sum_{l=1}^{\lfloor d/2 \rfloor} \sin\left(\frac{2\pi l}{d} \xi\right) = \frac{1}{2} \left[\cot\left(\frac{\pi \xi}{d}\right) - \frac{\cos(\pi \xi)}{\sin(\pi \xi / d)} \right]. \tag{4.41}$$

Introducing them into equation (4.39) and with the aid of some trigonometric formulas, one obtains

$$\begin{aligned} \sum_{l \in J} c_l \omega^{nl} &= \frac{1}{2} \left\{ \frac{\sin(\pi \xi)}{\sin(\pi \xi / d)} - 1 + \tan\left(\frac{\pi}{2m}\right) \left[\cot\left(\frac{\pi \xi}{d}\right) - \frac{\cos(\pi \xi)}{\sin(\pi \xi / d)} \right] \right\} \\ &= \frac{1}{2} \left\{ \tan\left(\frac{\pi}{2m}\right) \cot\left[\frac{\pi}{d}\left(n + \frac{1}{2m}\right)\right] - 1 \right\}. \end{aligned} \tag{4.42}$$

By replacing n with $-(n+1)$ in the above formula we then arrive at the expression for the sum in equation (4.38), that is,

$$\sum_{l\in J} c_l \omega^{-(n+1)l} = -\frac{1}{2}\left\{\tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(n+1-\frac{1}{2m}\right)\right]+1\right\}. \tag{4.43}$$

Finally, setting $n = \lfloor d/2 \rfloor = (d-1)/2$ in (4.42) one obtains a formula for S:

$$S = \frac{1}{2}\left\{1-\tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(\left\lfloor\frac{d}{2}\right\rfloor+\frac{1}{2m}\right)\right]\right\}. \tag{4.44}$$

Substituting equations (4.42), (4.43), and (4.44) into (4.36) and (4.38), we eventually obtain the coefficients α_n and β_n in the following form

$$\alpha_n = \frac{1}{2d}\tan\left(\frac{\pi}{2m}\right)\left\{\cot\left[\frac{\pi}{d}\left(n+\frac{1}{2m}\right)\right]-\cot\left[\frac{\pi}{d}\left(\left\lfloor\frac{d}{2}\right\rfloor+\frac{1}{2m}\right)\right]\right\} \tag{4.45}$$

and

$$\beta_n = \frac{1}{2d}\tan\left(\frac{\pi}{2m}\right)\left\{\cot\left[\frac{\pi}{d}\left(n+1-\frac{1}{2m}\right)\right]+\cot\left[\frac{\pi}{d}\left(\left\lfloor\frac{d}{2}\right\rfloor+\frac{1}{2m}\right)\right]\right\}. \tag{4.46}$$

with $n = 1, \ldots, \lfloor d/2 \rfloor$. As in expressions (4.22) and (4.23), the coefficients can be expressed using the function $g(x) = \cot(\frac{\pi}{d}(x+\frac{1}{2m}))$.

Even d. In this case, one can solve the system (4.34) analogously. The difference is, however, that (4.34) is the same equation for $l = -d/2$ and $l = d/2$, and therefore the system consists of $d-1$ equations for d variables. A non-unique solution is then expected.

Denoting $J_e = \{-(d-1)/2, \ldots, -1, 1, \ldots, d/2\}$ and following the same methodology as above with the set J replaced by J_e one arrives at α_n and β_n given by

$$\alpha_n = \frac{1}{2d}\left\{\tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(n+\frac{1}{2m}\right)\right]-1\right\}+\frac{1}{d}S \tag{4.47}$$

and

$$\beta_n = \frac{1}{2d}\left\{\tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(n+1-\frac{1}{2m}\right)\right]+1\right\}-\frac{1}{d}S, \tag{4.48}$$

where S is given by the same formula as in (4.37). Here, the quantity S (or, equivalently, one of the variables α_n or β_n) cannot be uniquely determined. We fix it in such a way that the resulting α_n and β_n are given by the same formulas as those in the odd d case, that is,

$$S = \frac{1}{2}\left\{1 - \tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(\left\lfloor\frac{d}{2}\right\rfloor + \frac{1}{2m}\right)\right]\right\}. \tag{4.49}$$

As a consequence the coefficients α_n and β_n are given by equations (4.22) and (4.23), both in the odd and even d cases.

$\widetilde{\mathbf{I}}_{\mathbf{m,d}}$ and $\mathbf{I}_{\mathbf{m,d}}$. It is finally worth mentioning that the values of the two Bell expressions—in terms of probabilities $I_{m,d}$ and in terms of generalised correlators $\widetilde{I}_{m,d}$ —are related in the following way:

$$\widetilde{I}_{m,d} = dI_{m,d} - 2mS, \tag{4.50}$$

where S is given by equation (4.49).

Special cases. Let us now consider two special cases of $d = 2$ and any m, and $m = 2$ and any d. In the first one, the Bell expression in the probability form simplifies to

$$I_{m,2} = \alpha_0\mathbb{P}_0 - \beta_0\mathbb{Q}_0 \tag{4.51}$$

where

$$\mathbb{P}_0 = \sum_{i=1}^{m}[P(A_i = B_i) + P(B_i = A_{i+1})],$$
$$\mathbb{Q}_0 = \sum_{i=1}^{m}[P(A_i = B_i - 1) + P(B_i = A_{i+1} - 1)] \tag{4.52}$$

and

$$\alpha_0 = \frac{1}{2\cos(\pi/2m)}, \qquad \beta_0 = 0. \tag{4.53}$$

Moreover, there is a unique coefficient a_1 and it simplifies to $1/[2\cos(\pi/2m)]$, so that in the correlator form our Bell expression for $d = 2$ becomes

$$\widetilde{I}_{m,2} = \frac{1}{2\cos(\pi/2m)}\left[\langle A_1B_1\rangle - \langle A_1B_m\rangle + \sum_{i=2}^{m}\left(\langle A_iB_i\rangle + \langle A_iB_{i-1}\rangle\right)\right], \tag{4.54}$$

This is the well-known chained Bell inequality [Pea70, BC90] that we studied in Chapter 3.

In the second case, i.e., that of $m = 2$ and any d, the Bell expression $I_{2,d}$ in the probability form is given by:

$$I_{2,d} = \sum_{k=0}^{\lfloor d/2 \rfloor - 1} \left(\alpha_k \mathbb{P}_k - \beta_k \mathbb{Q}_k \right), \tag{4.55}$$

with the expressions $\mathbb{P}_k$ and $\mathbb{Q}_k$ simplifying to

$$\mathbb{P}_k = P(A_1 = B_1 + k) + P(B_1 = A_2 + k) + P(A_2 = B_2 + k) + P(B_2 = A_1 + k + 1) \tag{4.56}$$

and

$$\mathbb{Q}_k = P(A_1 = B_1 - k - 1) + P(B_1 = A_2 - k - 1) + P(A_2 = B_2 - k - 1) + P(B_2 = A_1 - k), \tag{4.57}$$

where we have exploited the convention that $A_3 = A_1 + 1$. Then, the coefficients α_k and β_k are given by

$$\alpha_k = \frac{1}{2d}\left[g(k) + (-1)^d \tan\left(\frac{\pi}{4d}\right)\right], \quad \beta_k = \frac{1}{2d}\left[g\left(k + 1/2\right) - (-1)^d \tan\left(\frac{\pi}{4d}\right)\right], \tag{4.58}$$

with $g(k) = \cot[\pi(k + 1/4)/d]$. On the other hand, in the correlator form one obtains

$$\widetilde{I}_{2,d} = \sum_{l=1}^{d-1} \left[a_l \langle A_1^l B_1^{d-l} \rangle + a_l^* \omega^l \langle A_1^l B_2^{d-l} \rangle + a_l \langle A_2^l B_2^{d-l} \rangle + a_l^* \langle A_2^l B_1^{d-l} \rangle \right], \tag{4.59}$$

where $a_l = \omega^{(2l-d)/8}/\sqrt{2}$. It should be noted that this Bell inequality was previously studied in [SLK06] and [dV15], and, in particular in [dV15] and [LCL07] the maximal quantum violation was found using two different methods.

Conclusion

To sum up, our class of Bell expressions is given by $I_{m,d}$ (4.8) or equivalently by $\widetilde{I}_{m,d}$ (4.17), with coefficients (4.22) and (4.23). We arrived at this result by writing the most general Bell expression satisfying the symmetry of correlations stemming from CGLMP measurements, re-writing these Bell expressions in the simple form (4.17) through a change of variable on Bob's side, and then imposing the conditions (4.21) that take into account the symmetries of the maximally entangled state, as CHSH does for two binary measurements.

4.1.2. Properties of the Bell expressions

Our Bell expressions $\widetilde{I}_{m,d}$ have the following classical, quantum, and no-signalling bounds:

$$\begin{aligned}
\widetilde{\beta}_C &= (1/2)\tan(\pi/2m)\left\{(2m-1)g(0) - g(1-1/m)\right\} - m, &(4.60)\\
\widetilde{\beta}_Q &= m(d-1), &(4.61)\\
\widetilde{\beta}_{NS} &= m\tan(\pi/2m)\, g(0) - m, &(4.62)
\end{aligned}$$

with $g(x) = \cot(\pi(x+1/2m)/d)$. Given these values, we start by showing that $\widetilde{\beta}_C < \widetilde{\beta}_Q < \widetilde{\beta}_{NS}$ for any m and d, and we study their scaling for large values of m and d. Then, we present the detailed proofs of these three bounds, in Theorems 4.3, 4.6, and 4.7.

Ratios between the bounds

First, we have that the quantum bound is always higher than the classical bound, i.e. $\widetilde{\beta}_Q > \widetilde{\beta}_C$ for any $m, d \geq 2$. This means that all our Bell inequalities are nontrivial.

Lemma 4.1. *For any $m, d \geq 2$, the quantum bound of $\widetilde{I}_{m,d}$ is strictly larger than the classical one, that is,*

$$\widetilde{\beta}_Q / \widetilde{\beta}_C > 1. \tag{4.63}$$

Proof. We prove that $\widetilde{\beta}_Q - \widetilde{\beta}_C > 0$, which is equivalent to (4.63) since both bounds are larger than 0. This inequality can be written as:

$$2md\cot\left(\frac{\pi}{2m}\right) - 2m\cot\left(\frac{\pi}{2dm}\right) + \cot\left(\frac{\pi}{2dm}\right) + \cot\left(\frac{\pi}{d}\left(1-\frac{1}{2m}\right)\right) > 0. \tag{4.64}$$

If we define $a = 1/d$ and $x = \pi/2m$, it becomes:

$$ax\cot(a(\pi - x)) + a(x-\pi)\cot(ax) + \pi\cot(x) > 0, \tag{4.65}$$

for $0 < a \leq 1/2$ and $0 < x \leq \pi/4$. Since the first term is positive for these intervals, it suffices to show that

$$u(a,x) = a(x-\pi)\cot(ax) + \pi\cot(x) > 0. \tag{4.66}$$

Clearly, $u(a,x) \geq \min_a(u(a,x))$. This minimum corresponds to the limit $a \to 0$, since the derivative $\partial u(a,x)/\partial a$ of $u(a,x)$ with respect to a is strictly positive on the considered intervals of a and x. Indeed, it holds that

$$\frac{\partial u(a,x)}{\partial a} = (x-\pi)\cot(ax) - \frac{ax(x-\pi)}{\sin^2(ax)}, \tag{4.67}$$

which can be rewritten as

$$\frac{\partial u(a,x)}{\partial a} = \frac{\pi - x}{2\sin^2(ax)}\left[2ax - \sin(2ax)\right]. \tag{4.68}$$

Now, due to the fact that $y > \sin y$ for $0 < y \leq \pi/8$, one has that $2ax > \sin(2ax)$ for $0 < a \leq 1/2$ and $0 < x \leq \pi/4$, and therefore the right-hand side of equation (4.68) is strictly positive within the above intervals. Now, computing the limit of $u(a,x)$ when $a \to 0$, one obtains

$$\lim_{a\to 0} u(a,x) = 1 - \frac{\pi}{x} + \pi\cot(x). \tag{4.69}$$

It can be verified straightforwardly that this expression is strictly positive in the interval $0 < x \leq \pi/4$, by comparing the two functions $\pi\cot(x)$ and $\frac{\pi}{x} - 1$, and noticing that the former upper bounds the latter in the interval $0 < x \leq \pi/4$. Indeed, at $x = \pi/4$, we have that $\pi\cot(\pi/4) > 3$, and in this interval, both their derivatives are negative, with the derivative of the first function smaller than the derivative of the second one. Thus, $u(a,x) > 0$. □

Moreover, we have that the no-signalling bound is always strictly larger than the quantum bound, i.e. $\widetilde{\beta}_{NS} > \widetilde{\beta}_{Q}$ for any $m,d \geq 2$. Indeed:

Lemma 4.2. *For any $m,d \geq 2$, the no-signalling bound of $\tilde{I}_{m,d}$ is strictly larger than the quantum one, that is,*

$$\widetilde{\beta}_{NS}/\widetilde{\beta}_{Q} > 1. \tag{4.70}$$

Proof. Writing the ratio explicitely as $\widetilde{\beta}_{NS}/\widetilde{\beta}_{Q} = \frac{1}{d-1}(\tan\left(\frac{\pi}{2m}\right)\cot\left(\frac{\pi}{2dm}\right) - 1)$, it follows that it is enough to show that $\tan(\pi/2m)\cot(\pi/2dm) > d$. Let us prove a slightly simpler inequality:

$$\tan(\pi/2m) > d\tan(\pi/2dm). \tag{4.71}$$

To this end, we show that $\tan(ax) > a\tan(x)$ for any $0 < x \leq \pi/2a$ and any integer $a \geq 2$. We notice that for $x = 0$, $\tan(0) = a\tan(0)$, and that $[\tan(ax)]' \geq [a\tan(x)]' \geq 0$, meaning that both $\tan(ax)$ and $a\tan(x)$ are monotonically increasing functions and that the former grows faster than the latter. The inequality for the derivatives holds true because $\cos(x)$ is a monotonically decreasing function for $0 \leq x \leq \pi/2a$ which implies that $\cos(x) \geq \cos(ax)$. To complete the proof we note that $\tan(\pi/2m) = \tan[d(\pi/2dm)]$ and using $x = \pi/2dm$ and $a = d$, one can exploit the above inequality to obtain (4.71). This finally implies equation (4.70). □

Scaling of the bounds

Let us continue our study of the ratios between the bounds of our Bell expressions by considering their asymptotic behaviour for large numbers of inputs m and outputs d. This can be of interest when studying applications in device-independent protocols, for instance. Let us start with the quantity:

$$\frac{\widetilde{\beta}_Q}{\widetilde{\beta}_C} = \frac{2m(d-1)}{\tan\left(\frac{\pi}{2m}\right)\left[(2m-1)\cot\left(\frac{\pi}{2dm}\right) - \cot\left(\frac{\pi}{d}(1-\frac{1}{2m})\right)\right] - 2m} \tag{4.72}$$

which is the ratio between the quantum and classical bounds. We also consider the ratio between the no-signalling and quantum bounds, which is:

$$\frac{\widetilde{\beta}_{NS}}{\widetilde{\beta}_Q} = \frac{\tan\left(\frac{\pi}{2m}\right)\cot\left(\frac{\pi}{2dm}\right) - 1}{d-1}. \tag{4.73}$$

To observe the behaviour of these quantities for high number of inputs m and outputs d, we can use the Taylor series expansion in two variables, $1/m$ and $1/d$, and keep the dominant terms. We obtain:

$$\frac{\widetilde{\beta}_Q}{\widetilde{\beta}_C} = 1 + \frac{1}{2m} - \frac{\pi^2 - 6}{12m^2} + \cdots \tag{4.74}$$

$$\frac{\widetilde{\beta}_{NS}}{\widetilde{\beta}_Q} = 1 + \frac{\pi^2/12 - \pi^2/12d^2}{m^2} + \cdots \tag{4.75}$$

Thus, when the parameters m and d are of the same order and both very large, i.e. $m = \Theta(d)$, both ratios tend to 1. It is interesting to consider how fast the bounds tend towards each other: since the ratio between the no-signalling and quantum bounds lacks a term in $1/m$, it is clear that the quantum bound approaches the no-signalling bound faster than the classical bound approaches the quantum bound.

If we fix the number of outputs d and consider the limit of a large number of inputs m, the ratios still tend to 1. However, if we fix m and consider the limit of large d, both ratios tend to constants which are a bit bigger than 1. They are :

$$\lim_{d\to\infty} \widetilde{\beta}_Q/\widetilde{\beta}_C = \frac{(2m-1)\,\pi\cot(\pi/2m)}{4m(m-1)} \tag{4.76}$$

$$\lim_{d\to\infty} \widetilde{\beta}_{NS}/\widetilde{\beta}_Q = \frac{2}{\pi} m \tan\left(\frac{\pi}{2m}\right). \tag{4.77}$$

It is worth mentioning that both functions of m appearing on the right-hand sides of the above formulas attain their maxima for $m = 2$ which are $4/\pi$ and

$3\pi/8$, respectively. To give the reader more insight, we present in Tables A.1 and A.2 the numerical values of these ratios for low values of m and d (all Tables can be found in Appendix A).

Classical bound of the inequalities

We are now ready to move on to the proofs of the bounds of our Bell expressions. We start with the classical bound. As announced (4.60), we have:

Theorem 4.3. *The classical bound of* $\widetilde{I}_{m,d}$ *is given by*

$$\widetilde{\beta}_C = (1/2)\tan(\pi/2m)\left\{(2m-1)g(0) - g(1-1/m)\right\} - m, \tag{4.78}$$

with $g(x) = \cot(\pi(x+1/2m)/d)$.

In order to prove this bound, let us simplify the form of the problem. We start with our Bell expression in the probability form $I_{m,d}$ and note that we can rewrite it as:

$$I_{m,d} = \sum_{k=0}^{d-1} \alpha_k \sum_{i=1}^{m} [P(A_i = B_i + k) + P(B_i = A_{i+1} + k)], \tag{4.79}$$

with $A_{m+1} = A_1 + 1$. This is possible because of the form (4.22) and (4.23) of coefficients α_k and β_k. Indeed, since $\alpha_k = -\beta_{d-k-1}$, the terms of the sum which were attached to the β_k coefficients can be shifted to indices $k = \lfloor d/2 \rfloor, \ldots, d-1$ and now associated to an α_k. In the odd case, we should in principle impose that the term $k = \lfloor d/2 \rfloor$ disappears, but it happens naturally since $\alpha_{\lfloor d/2 \rfloor} = 0$.

As mentioned in Chapter 2, finding the classical bound of a Bell expression reduces to computing the optimal deterministic strategy. Following this assumption of determinism, we describe the difference between the outcomes associated to A_x and B_y by assigning one value q such that $P(A_x = B_y + k) = \delta_{kq}$. As q depends on inputs x and y but not all pairs of A_x and B_y appear in the Bell expression, we thus define $2m$ variables $q_i \in \{0, 1 \ldots, d-1\}$ such that:

$$\begin{aligned}
A_1 - B_1 &= q_1, \\
B_1 - A_2 &= q_2, \\
A_2 - B_2 &= q_3, \\
&\vdots \\
A_m - B_m &= q_{2m-1}, \\
B_m - A_1 &= q_{2m} + 1.
\end{aligned} \tag{4.80}$$

Due to the chained character of these equations, q_{2m} must obey a superselection rule involving the other q_i's, which is

$$q_{2m} = -1 - \sum_{i=1}^{2m-1} q_i, \tag{4.81}$$

where the sum is modulo d. Since the dependence of the coefficients α_k on k is only through the cotangent function, we can further simplify the problem of finding the classical bound, thus rephrasing Theorem 4.3:

Theorem 4.3. *Let*

$$\hat{\alpha}_k := \cot\left[\frac{\pi}{d}\left(k + \frac{1}{2m}\right)\right],$$

and let

$$\hat{\beta}_C := \max_{0 \leq q_1, \ldots, q_{2m-1} < d} \left(\sum_{i=1}^{2m-1} \hat{\alpha}_{q_i} + \hat{\alpha}_{-1-\sum_{i=1}^{2m-1} q_i \mod d} \right). \tag{4.82}$$

Then, $\hat{\beta}_C = (2m-1)\hat{\alpha}_0 + \hat{\alpha}_{d-1}$.

This means that the optimal deterministic strategy is to set to one $2m-1$ of the terms $P(A_x = B_y + z)$ multiplied by α_0 and a single term multiplied by β_0, and the remaining terms to zero. To recover expression $\widetilde{\beta}_C$ from $\hat{\beta}_C$, one needs to reintroduce the constant factors appearing in the definition of α_k and use equation (4.50). To prove the theorem, we first demonstrate two lemmas. We will be assuming that $m \geq 2$ and $d \geq 2$. Although these are not tight conditions to prove our results, they are in any case satisfied by the definition of a Bell test.

Lemma 4.4. *Let* $g(x) = \cot[\pi(x + \frac{1}{2m})/d]$. *For all* x, y *satisfying* $0 \leq x < y < d - \frac{1}{2m}$, *we have*

$$(1 + 2mx)g(x) > (1 + 2my)g(y). \tag{4.83}$$

Proof. Let us consider the function $f(z) = z \cot z$, which is strictly decreasing in the interval $0 < z < \pi$. This can be shown for instance by noting that f is holomorphic and by studying the sign of the coefficients of its Laurent series in a ball of radius π centered at $z = 0$. Thus, for every $c \in (0, \pi)$, $f(c) > f(z)$ for all $c < z < \pi$. In particular, we can pick $c = \frac{\pi}{2dm}(1 + 2mx)$ so that:

$$\frac{\pi}{2dm}(1 + 2mx)\cot\left(\frac{\pi}{2dm}(1 + 2mx)\right) > zf(z), \tag{4.84}$$

for $\frac{\pi}{2dm}(1+2mx) < z < \pi$. By introducing the change of variables $z = \frac{\pi}{2dm}(1+2my)$, equation (4.83) follows. Note that for integer values of x and y, namely k and l, Lemma 4.4 becomes:

$$(1+2mk)\hat{\alpha}_k > (1+2ml)\hat{\alpha}_l, \qquad \forall 0 \leq k < l < d. \tag{4.85}$$

□

Lemma 4.5. *For integer indices k, l, p such that $0 < k, l < d$ and $0 \leq p < d$, we have:*

$$\hat{\alpha}_0 + \hat{\alpha}_p > \hat{\alpha}_k + \hat{\alpha}_l. \tag{4.86}$$

Proof. Because all the α's are ordered $\hat{\alpha}_0 > \hat{\alpha}_1 > \hat{\alpha}_2 > \cdots > \hat{\alpha}_{d-1}$, we have that $\hat{\alpha}_0 + \hat{\alpha}_p \geq \hat{\alpha}_0 + \hat{\alpha}_{d-1}$ and $\hat{\alpha}_1 + \hat{\alpha}_1 \geq \hat{\alpha}_k + \hat{\alpha}_l$. Hence, it suffices to prove that

$$\hat{\alpha}_0 + \hat{\alpha}_{d-1} > 2\hat{\alpha}_1. \tag{4.87}$$

Let us rewrite this inequality using function g. To this end, we note that the symmetry of the function $\cot(x) = -\cot(-x)$ translates to $g(x)$ in the following manner: $g(x) = -g(-x - 1/m)$. Thus, in order to prove (4.87), we need to show:

$$g(0) > 2g(1) + g(1 - 1/m). \tag{4.88}$$

Using Lemma 4.4 twice, we can express that:

$$g(0) > (2m-1)g(1-1/m) > g(1-1/m) + 2(m-1)\frac{(1+2m)}{(2m-1)}g(1). \tag{4.89}$$

To obtain the second inequality, one of the $2m-1$ terms was isolated, and Lemma 4.4 was applied only on the remaining $2(m-1)$ terms. The minimum of $2(m-1)(1+2m)/(2m-1)$ is found for $m = 2$ and it is equal to $10/3$. Since $g(1)$ is positive, and $10/3 > 2$, we can conclude that $g(0) > g(1-1/m) + 2g(1)$, which is exactly relation (4.88). □

Proof of Theorem 4.3. To demonstrate the theorem, we employ a dynamic programming procedure which allows us to rewrite equation (4.82) as a chain of maximisations, each over a single variable. Let us first define

$$h(x) = \max_{0 \leq y < d} \left(\hat{\alpha}_y + \hat{\alpha}_{-1-x-y}\right), \tag{4.90}$$

where the indices are taken to be modulo d. As a direct consequence of Lemma 4.5, $h(x) = \hat{\alpha}_0 + \hat{\alpha}_{-1-x}$. Indeed, the lemma implies that $\hat{\alpha}_0 + \hat{\alpha}_{-1-x} > \hat{\alpha}_y + \hat{\alpha}_{-1-x-y}$ if $y > 0$ and $x \neq d-1-y$. For the cases where $y = 0$ or $x = d-1-y$, the maximum is directly attained. This allows us to write the classical bound as:

$$\hat{\beta}_C = \max_{q_1}\left(\hat{\alpha}_{q_1} + \max_{q_2}\left(\hat{\alpha}_{q_2} + \ldots + \max_{q_{2m-2}}\left(\hat{\alpha}_{q_{2m-2}} + h\left(\sum_{i=1}^{2m-2} q_i\right)\right)\ldots\right)\right). \tag{4.91}$$

Using the properties of h, we find that

$$\max_{q_k}\left[\hat{\alpha}_{q_k} + h\left(\sum_{i=1}^{k} q_i\right)\right] = \hat{\alpha}_0 + h\left(\sum_{i=1}^{k-1} q_i\right) \tag{4.92}$$

for all k. By applying this step $2(m-1)$ times to expression (4.91), we obtain:

$$\hat{\beta}_C = (2m-2)\hat{\alpha}_0 + h(0) = (2m-1)\hat{\alpha}_0 + \hat{\alpha}_{-1}. \tag{4.93}$$

□

Importantly, the resulting Bell inequality $\widetilde{I}_{m,d} \leq \widetilde{\beta}_C$ is violated by quantum theory – one can reach the value $\widetilde{I}_{m,d} = m(d-1)$ by applying the CGLMP measurements on $|\phi_d^+\rangle$. This is seen by using (4.21), the unitarity of A_i^k, and the symmetries of the maximally entangled states (4.20). Then, all the correlators in (4.17) equal one, yielding the quantum violation of $m(d-1)$. As announced in (4.61), this violation is optimal and defines the tight Tsirelson bound of $\widetilde{I}_{m,d}$. We prove this result below.

Tsirelson bound of the inequalities

Theorem 4.6. *The Tsirelson bound of $\widetilde{I}_{m,d}$ is given by*

$$\widetilde{\beta}_Q = m(d-1). \tag{4.94}$$

Proof. We give an SOS decomposition to prove the maximal quantum violation of $\widetilde{I}_{m,d}$ (see expression (2.20)). Concretely, we show that the identity

$$\widetilde{\beta}_Q \mathbb{1} - \mathcal{B} = \frac{1}{2}\sum_{i=1}^{m}\sum_{k=1}^{d-1} P_{ik}^\dagger P_{ik} + \frac{1}{2}\sum_{i=1}^{m-2}\sum_{k=1}^{d-1} T_{ik}^\dagger T_{ik}, \tag{4.95}$$

is valid independently of the choice of A_i^k and B_i^k. The operators are thus not specified. Here, $P_{ik} = \mathbb{1} \otimes \bar{B}_i^k - (A_i^k)^\dagger \otimes \mathbb{1}$, and

$$T_{ik} = \mu_{i,k} B_2^{d-k} + \nu_{i,k} B_{i+2}^{d-k} + \tau_{i,k} B_{i+3}^{d-k}, \tag{4.96}$$

where the coefficients μ_{ik}, ν_{ik} and τ_{ik} are given by

$$\begin{aligned}
\mu_{i,k} &= \frac{\omega^{(i+1)(d-2k)/2m}}{2\cos(\pi/2m)}\frac{\sin(\pi/m)}{\sqrt{\sin(\pi i/m)\sin\left[\pi(i+1)/m\right]}},\\
\nu_{i,k} &= -\frac{\omega^{(d-2k)/2m}}{2\cos(\pi/2m)}\sqrt{\frac{\sin\left[\pi(i+1)/m\right]}{\sin(\pi i/m)}},\\
\tau_{i,k} &= \frac{1}{2\cos(\pi/2m)}\sqrt{\frac{\sin(\pi i/m)}{\sin\left[\pi(i+1)/m\right]}} = -\frac{\omega^{(d-2k)/2m}}{4\cos^2(\pi/2m)}\nu_{ik}^{-1}, \qquad (4.97)
\end{aligned}$$

for $i=1,\ldots,m-3$ and $k=1,\ldots,d-1$, while for $i=m-2$ and $k=1,\ldots,d-1$ they are given by

$$\begin{aligned}
\mu_{m-2,k} &= -\frac{\omega^{-(d-2k)/2m}}{2\sqrt{2}\cos(\pi/2m)\sqrt{\cos(\pi/m)}},\\
\nu_{m-2,k} &= -\frac{\omega^{k}\omega^{(d-2k)/2m}}{2\sqrt{2}\cos(\pi/2m)\sqrt{\cos(\pi/m)}},\\
\tau_{m-2,k} &= \frac{\sqrt{\cos(\pi/m)}}{\sqrt{2}\cos(\pi/2m)}. \qquad (4.98)
\end{aligned}$$

Now, in order to check the validity of the SOS decomposition (4.95) let us first introduce the explicit form of P_{ik} into the first term of the right-hand side of (4.95), which gives

$$\sum_{i=1}^{m}\sum_{k=1}^{d-1}P_{ik}^{\dagger}P_{ik} = \widetilde{\beta}_Q\mathbb{1} - 2\mathcal{B} + \mathbb{1}\otimes\sum_{i=1}^{m}\sum_{k=1}^{d-1}(\bar{B}_i^k)^{\dagger}(\bar{B}_i^k), \qquad (4.99)$$

where we have used the fact that the Bell operator $\mathcal{B}$ is Hermitian. Let us then introduce the explicit form of the operators T_{ik} into the last term of the right-hand side of (4.95), which, after some algebra, leads us to

$$\begin{aligned}
&\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}T_{ik}^{\dagger}T_{ik}\\
&= \sum_{i=1}^{m-2}\sum_{k=1}^{d-1}\left(|\mu_{i,k}|^2+|\nu_{i,k}|^2+|\tau_{i,k}|^2\right)\mathbb{1}\\
&\quad+\sum_{k=1}^{d-1}\left[\mu_{1,k}^{*}\nu_{1,k}(B_2^{d-k})^{\dagger}(B_3^{d-k})+\mu_{1,k}\nu_{1,k}^{*}(B_3^{d-k})^{\dagger}(B_2^{d-k})\right]
\end{aligned}$$

$$
\begin{aligned}
&+\sum_{k=1}^{d-1}\left[\mu^*_{m-2,k}\tau_{m-2,k}(B_2^{d-k})^\dagger(B_1^{d-k})+\mu_{m-2,k}\tau^*_{m-2,k}(B_1^{d-k})^\dagger(B_2^{d-k})\right]\\
&+\sum_{i=1}^{m-3}\sum_{k=1}^{d-1}\Big[(\mu^*_{i,k}\tau_{i,k}+\mu^*_{i+1,k}\nu_{i+1,k})(B_2^{d-k})^\dagger(B_{i+3}^{d-k})\\
&\qquad\qquad+(\mu_{i,k}\tau^*_{i,k}+\mu_{i+1,k}\nu^*_{i+1,k})(B_{i+3}^{d-k})^\dagger(B_2^{d-k})\Big]\\
&+\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}\left[\nu^*_{i,k}\tau_{i,k}(B_{i+2}^{d-k})^\dagger(B_{i+3}^{d-k})+\nu_{i,k}\tau^*_{i,k}(B_{i+3}^{d-k})^\dagger(B_{i+2}^{d-k})\right].
\end{aligned}
\tag{4.100}
$$

Now, it follows from equations (4.154) and (4.155) that $\mu^*_{i,k}\tau_{i,k}+\mu^*_{i+1,k}\nu_{i+1,k}=0$ for $i=1,\ldots,m-3$ and $k=1,\ldots,d-1$, which means that the fourth and fifth lines in the above vanish. Then, one notices that $\mu^*_{1,k}\nu_{1,k}=\mu_{m-2,k}\tau^*_{m-2,k}=\nu^*_{i,k}\tau_{i,k}=-a_k^2$ for $i=1,\ldots,m-3$ and $k=1,\ldots,d-1$, and $\nu_{m-2,k}\tau^*_{m-2,k}=-\omega^k(a_k^*)^2$ for $k=1,\ldots,d-1$, where, as before, $a_k=\omega^{-(d-2k)/4m}/[2\cos(\pi/2m)]$. Therefore, the remaining terms on the right-hand side of (4.100) can be wrapped up as

$$
\begin{aligned}
\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}T^\dagger_{ik}T_{ik} \;=\;& \sum_{i=1}^{m-2}\sum_{k=1}^{d-1}\left(|\mu_{ik}|^2+|\nu_{ik}|^2+|\tau_{ik}|^2\right)\mathbb{1}\\
&-\sum_{i=1}^{m-1}\sum_{k=1}^{d-1}\left[a_k^2(B_i^{d-k})^\dagger(B_{i+1}^{d-k})+(a_k^*)^2(B_{i+1}^{d-k})^\dagger(B_i^{d-k})\right]\\
&-\sum_{k=1}^{d-1}\left[\omega^k(a_k^*)^2(B_1^{d-k})^\dagger(B_m^{d-k})+\omega^{-k}a_k^2(B_m^{d-k})^\dagger(B_1^{d-k})\right].
\end{aligned}
\tag{4.101}
$$

By substituting equations (4.99) and (4.101) into (4.95) and exploiting the explicit form of the operators $\bar{B}_i^k$, one obtains

$$
\begin{aligned}
&\frac{1}{2}\sum_{i=1}^{m}\sum_{k=1}^{d-1}P^\dagger_{ik}P_{ik}+\frac{1}{2}\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}T^\dagger_{ik}T_{ik}\\
&=\frac{1}{2}\widetilde{\beta}_Q\mathbb{1}-\mathcal{B}+\sum_{k=1}^{d-1}\left[m|a_k|^2+\frac{1}{2}\sum_{i=1}^{m-2}\left(|\mu_{i,k}|^2+|\nu_{i,k}|^2+|\tau_{i,k}|^2\right)\right]\mathbb{1}.
\end{aligned}
\tag{4.102}
$$

One can then verify that the last two terms in the above formula amount to $(1/2)\widetilde{\beta}_Q=(1/2)m(d-1)$, which completes the proof. □

Before moving on to the no-signalling bound, let us elaborate on how the SOS works in the case of two measurements, $m = 2$. In fact, this gives us a motivation for the choice of conditions (4.21) that led to the coefficients α_k and β_k. For $m = 2$, the second part of the SOS decomposition (4.95) vanishes. For the optimal CGLMP measurements both sides of (4.95) must yield zero when applied to $|\phi_d^+\rangle$, which stems from conditions (4.20) and (4.21). This allows one to grasp the intuition behind conditions (4.21), i.e., they allow one to construct in a quite direct way an SOS decomposition (4.95), in which all operators P_{ik} are polynomials of the measurement operators A_i^k and B_i^k of order one, significantly facilitating the computation of the Tsirelson bound. For the CHSH Bell inequality, one observes the same effect, as these same properties of the optimal state and measurements allow the Bell operator $\mathcal{B}_{\mathrm{CHSH}} = A_1 \otimes B_1 + A_1 \otimes B_2 + A_2 \otimes B_1 - A_2 \otimes B_2$ to have the decomposition:

$$2\sqrt{2}\mathbb{1} - \mathcal{B}_{\mathrm{CHSH}} = (P_1^\dagger P_1 + P_2^\dagger P_2)/\sqrt{2}, \tag{4.103}$$

with $P_1 = (1/\sqrt{2})\mathbb{1} \otimes (B_1 + B_2) - A_1 \otimes \mathbb{1}$, and $P_2 = (1/\sqrt{2})\mathbb{1} \otimes (B_1 - B_2) - A_2 \otimes \mathbb{1}$. Thus, our construction generalises this quantum aspect of the CHSH Bell operator. For larger number of measurements, $m > 2$, the first part of the SOS decomposition is not enough and one has to add "by hand" the extra term in which all T_{ik}'s are also of order one in B_i^k.

No-signalling bound of the inequalities

As announced in (4.62), we have:

Theorem 4.7. *The no-signalling bound of $\widetilde{I}_{m,d}$ is given by*

$$\widetilde{\beta}_{NS} = m \tan(\pi/2m)\, g(0) - m, \tag{4.104}$$

with $g(x) = \cot(\pi(x + 1/2m)/d)$.

Proof. As for the classical bound of our inequalities, we start from the Bell expression written as in (4.79):

$$I_{m,d} = \sum_{k=0}^{d-1} \alpha_k \sum_{i=1}^{m} [P(A_i = B_i + k) + P(B_i = A_{i+1} + k)], \tag{4.105}$$

with $A_{m+1} = A_1 + 1$. Following considerations from the proof the classical bound, it is clear that the coefficient α_0 is the largest of the sum. Thus, the algebraic bound of the Bell expression $I_{m,d}$ is $2m\alpha_0$. We now show that there exists a no-signalling behaviour that reaches the algebraic bound, which is thus also the no-signalling bound. Let us recall the no-signalling conditions for a probability distribution:

$$\begin{aligned}\sum_b P(A_x = a, B_y = b) &= \sum_b P(A_x = a, B_{y'} = b) \qquad \forall a, x, y, y' \\ \sum_a P(A_x = a, B_y = b) &= \sum_a P(A_{x'} = a, B_y = b) \qquad \forall b, y, x, x', \end{aligned} \tag{4.106}$$

which were introduced in Chapter 2. The behaviour that we present is the following. For inputs x and y such that $x = y$ or $x = y + 1$:

$$P(A_y = a, B_y = b) = P(A_{y+1} = a, B_y = b) = \begin{cases} 1/d & \text{if} \quad a = b \\ 0 & \text{if} \quad a \neq b. \end{cases} \tag{4.107}$$

There is a special case for $x = 1$ and $y = m$:

$$P(A_1 = a, B_m = b) = \begin{cases} 1/d & \text{if} \quad a = b - 1 \\ 0 & \text{if} \quad a \neq b - 1, \end{cases} \tag{4.108}$$

where the addition is modulo d. For all the other input combinations (i.e. the ones not appearing in the inequalities), we have:

$$P(A_x = a, B_y = b) = 1/d^2 \qquad \forall a, b. \tag{4.109}$$

One can verify that this distribution satisfies conditions (4.106). Thus, the no-signalling bound of $I_{m,d}$ is $\beta_{NS} = 2m\alpha_0$. To obtain the value $\widetilde{\beta}_{NS}$ of (4.104), it suffices to write explicitly $2m\alpha_0$ and to use relation (4.50). □

4.1.3. Applications to device-independent protocols

Now that we have thoroughly studied the properties of our Bell inequalities, let us discuss their applications to DI protocols. We proceed by considering examples.

Self-testing

A natural application of our Bell inequalities is self-testing. We apply the numerical SWAP method presented in Section 2.3.4 to $\widetilde{I}_{m,d}$ for the simplest case $m = 2$ and $d = 3$. The results are plotted in Figure 4.1, and show that one can self-test the maximally entangled state of two qutrits $|\phi_3^+\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$ with our inequalities.

An open question is whether one can generalise this result to any dimension (or at least higher dimension). The behaviour $\vec{p}$ maximally violating $\widetilde{I}_{m,d}$ would

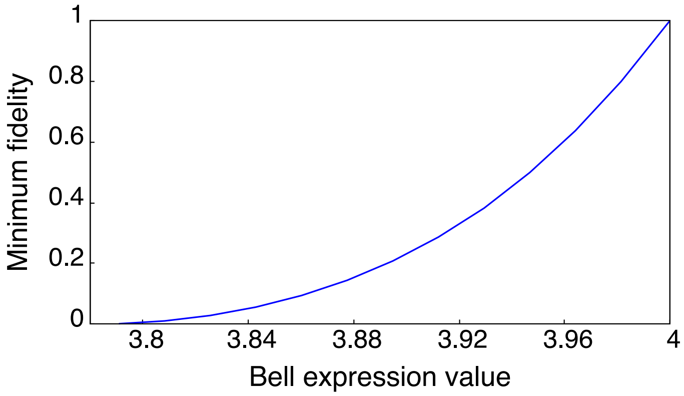

Figure 4.1.: Minimum fidelity of the physical state to the reference state $|\phi_3^+\rangle$, as a function of the violation of $\widetilde{I}_{3,2}$. At the maximal violation 4, the fidelity is equal to 1, meaning that the quantum state used in the Bell experiment must be maximally entangled. The numerical method that we used does not yield a positive lower bound on the fidelity below $\widetilde{I}_{3,2} \approx 3.79$ (for comparison, the classical bound is $\widetilde{I}_{3,2} \leq (1+3\sqrt{3})/2 \approx 3.01$).

then be proven to be unique in the general case, and our inequalities could find applications in DI random number generation protocols. Indeed, our inequalities possess enough symmetries so that the method of [DPA13] could be applied to guarantee a dit of perfect randomness. This, by increasing the dimension d, would eventually result in unbounded randomness expansion.

Device-independent quantum key distribution

Our inequalities could also find applications in DIQKD. An advantage that our inequalities have over CGLMP in that scenario [HP13] is that, as said before, the maximal violation is obtained for the maximally entangled state. This state can produce perfect correlations between the users, which reduces the error-correcting phase of the protocol and can lead to better key generation rates.

Let us study an example: we follow the protocol presented in Section 2.3.3, for the simple scenario of $m = 2$ and $d = 3$. Alice and Bob test the violation of a Bell inequality (CGLMP for three outcomes, or ours, $I_{2,3}$) to certify the security of their outcomes. To generate the key, Alice uses her first setting A_1 and Bob a third measurement B_3 which is chosen to be the same as A_1 (defined in expression (4.14)). A bound on the key rate can then be computed according to formula (2.32)

$$K \geq H_{\min}^{x^*=1} - H(A_1|B_3). \tag{4.110}$$

The local guessing probability for the first setting is found to be equal to 1/3 in both cases at the maximal violation, which means that the min-entropy is $H_{\min}^1 = 1$ if we measure in trits (i.e. $H_{\min} = -\log_3 P_{\text{guess}}$). The second term gives for our inequalities $H(A_1|B_3) = 0$, since the state is the maximally entangled state and the correlations are thus perfect. A numerical optimisation on the measurement B_3 shows that there is no better choice for the CGLMP case than to indeed set B_3 to be the same as A_1. This second term is larger than zero $H(A_1|B_3) = 0.0618$ for CGLMP, since the optimal state is $|\psi_\gamma\rangle = (|00\rangle + \gamma|11\rangle + |22\rangle)/\sqrt{2+\gamma^2}$, with $\gamma = (\sqrt{11} - \sqrt{3})/2$. We thus find the following bounds on the key rates, in the ideal case:

$$K_{I_{2,3}} \geq 1, \tag{4.111}$$

$$K_{\text{CGLMP}} \geq 0.9382, \tag{4.112}$$

i.e. our inequality guarantees a key rate of 1 trit or 1.58 bits, while CGLMP guarantees a key rate of 0.9382 trits, or 1.49 bits.

Let us now consider the effect of white noise on this example. The noise is described by parameter η, and affects the optimal state $|\psi\rangle$ as:

$$\rho' = (1-\eta)|\psi\rangle\langle\psi| + \eta\frac{\mathbb{I}}{d^2}, \tag{4.113}$$

which leads to a non-maximal violation of the Bell inequality. The results are shown in Figure 4.2. Up until a noise level of $\eta \approx 0.0428$, i.e. 4.3 percent, our inequality leads to a higher key rate than CGLMP. Around $\eta \approx 0.102$, the key rate has fallen to 0 for both inequalities. Note that our bounds on the guessing probability were obtained numerically, thus this method is limited to simple scenarios. Proving such bounds analytically remains an open question, both for CGLMP and for our inequalities. Nevertheless, we can make some conjectures about the general case.

In particular, when the maximal violation is observed without any noise, we expect to find $H_{\min}^{x^*} = 1$. This conjecture allows us to directly connect the key rate to the quantum mutual information $I(A:B)$:

$$K^{\eta=0} \geq H_{\min}^{x^*} - H(A_{x^*}|B_{y^*}) = H(A_{x^*}) - H(A_{x^*}|B_{y^*}) \equiv I(A_{x^*} : B_{y^*}). \tag{4.114}$$

One can compute the mutual information for the case when projective measurements are applied on a bipartite pure state $|\psi_{AB}\rangle$. It is straightforward to

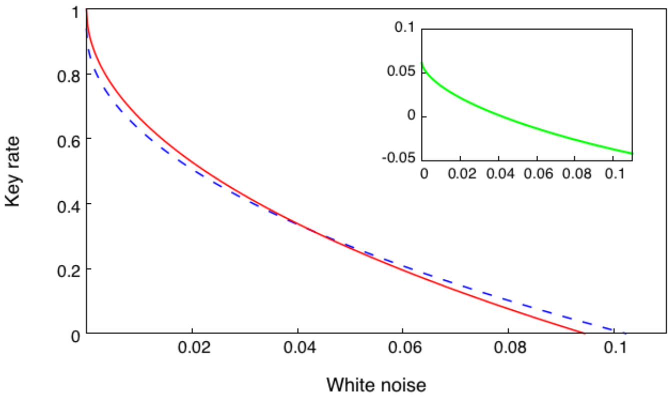

Figure 4.2.: Asymptotic key rate K as a function of the white noise η. The red curve corresponds to the key rate certified with our inequality $I_{2,3}$, while the blue dashed curve corresponds to key rate with CGLMP. On the top right, the difference between the two key rates is plotted as a function of the white noise η.

see that the mutual information is upper bounded by the entanglement entropy of the state, $I(A:B) \leq E(|\psi_{AB}\rangle)$. For a state $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, the entropy of entanglement [Bru02] is defined as

$$E(|\psi_{AB}\rangle) = -\mathrm{Tr}(\rho_A \mathrm{log} \rho_A) = -\mathrm{Tr}(\rho_B \mathrm{log} \rho_B), \tag{4.115}$$

with the reduced density matrices $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B = \mathrm{Tr}_A(\rho_{AB})$ (here we use logarithm to base d). The bound is tight, i.e. $I(A:B) = E(|\psi_{AB}\rangle)$, when the measurements are performed in the Schmidt basis of the state, which corresponds to the best possible choice of measurements x^*, y^* to generate a secret key, given that state. Note that implementing these Schmidt basis measurements in the protocol may not be possible, depending on the Bell inequality used and its own optimal measurements. In [ZG08], the authors investigated numerically the states that maximally violate the CGLMP inequalities, and they found that their entanglement entropy decreases as a function of d. On the other hand, the entanglement entropy of the maximally entangled state is equal to 1 and independent of the dimension. Since this quantity upper bounds the mutual information, these results indicate that the key rate for $\eta = 0$ would decrease monotonically with d for the CGLMP optimal states, while our key rate would remain equal to 1.

In conclusion, we can conjecture in the noiseless case that the advantage of our inequality over CGLMP grows with the dimension of the systems used for

DIQKD. Moreover, note that maximally entangled states can be much simpler to prepare experimentally than fine-tuned partially entangled states such as the ones maximally violating CGLMP, depending on the setup. However, we are aware that these observations are only preliminary – it would be interesting to confirm these conjectures in a future work focused on DIQKD.

4.1.4. Discussion: structure of the quantum set

There is an aspect of our results that is linked to the fundamental question of the study of the set of quantum correlations. Indeed, a feature of our inequalities worth highlighting is that their Tsirelson bound corresponds to the bound obtained using the NPA hierarchy at the first level $\mathcal{Q}_1$. This is a rare property, which has been previously observed only for XOR games (see, e.g., [Weh06]) and follows from our SOS decomposition (see (4.95)). Indeed, the degree of an optimal SOS decomposition for a Bell operator is directly linked to the level of the NPA hierarchy at which the quantum bound is obtained [PNA10]. An SOS of degree one, as in our case, corresponds to the first level $\mathcal{Q}_1$. This means that the boundaries of the sets $\mathcal{Q}$ and $\mathcal{Q}_1$ intersect at the maximal violation of our inequalities. This observation along with the results of [dV15] seem to suggest that the boundaries of $\mathcal{Q}$ and $\mathcal{Q}_1$ intersect at points that correspond to the maximal violation of Bell inequalities attained by maximally entangled states. Note, however, that the opposite implication is not true. That is, there exist Bell inequalities whose maximal violation by the maximally entangled state does not correspond to the intersection of $\mathcal{Q}$ and $\mathcal{Q}_1$ [LLD09]. The above property, if proven in general, could be used to characterise $\mathcal{Q}_1$.

4.2. Extension to the multipartite case

In this section, we present the extension of our results to the case of N parties. The form of the Bell expressions can be generalised in a quite straightforward way, using a procedure from [AGCA12]. The state maximally violating the Bell expression becomes the generalised N-partite GHZ state (2.4):

$$|\mathrm{GHZ}_{N,d}\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\dots i\rangle. \tag{4.116}$$

The quantum, no-signalling, and Svetlichny bounds can be obtained analytically as a function of N, m and d. However, the optimisation problem for the classical bound becomes much harder to solve – we provide the value of the classical bound for a few values of N, m, d only.

4.2.1. Generalisation of the Bell expressions

Aolita *et al.* introduced a generalisation of the CGLMP/BKP expressions for many parties in [AGCA12]. Their Bell inequalities can be rewritten in the following form:

$$I_{AGCA} = \sum_{k=0}^{\lfloor d/2 \rfloor -1} \left[\left(1 - \frac{2k}{d-1}\right) \left(\mathbb{P}_k^N - \mathbb{Q}_k^N\right) \right] \tag{4.117}$$

where $\mathbb{P}_k^N$ and $\mathbb{Q}_k^N$ are expressions given explicitly by

$$\begin{aligned} \mathbb{P}_k^N &= \sum_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}=1}^{m} \left[P(X_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = k) + P(\overline{X}_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = k) \right] \\ \mathbb{Q}_k^N &= \sum_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}=1}^{m} \left[P(X_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = -k-1) + P(\overline{X}_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = -k-1) \right], \end{aligned} \tag{4.118}$$

where X and $\overline{X}$ are linear combinations of $A_{x_j}^{(j)}$ defined as

$$X_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = \sum_{j=1}^{N} (-1)^{j-1} A^{(j)}_{\tilde{x}_{j-1}+\tilde{x}_j-1} \tag{4.119}$$

where (j) denotes the jth party and $x_j = \tilde{x}_{j-1} + \tilde{x}_j - 1$ is the measurement input, with the convention that $\tilde{x}_0 = \tilde{x}_N = 1$, so that the first and last inputs are $x_1 = \tilde{x}_1$ and $x_N = \tilde{x}_{N-1}$. Similarly:

$$\overline{X}_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = \sum_{j=1}^{N} (-1)^{j} A^{(j)}_{\tilde{x}_{j-1}+\tilde{x}_j-1} \tag{4.120}$$

with $\tilde{x}_0 = 2$ and $\tilde{x}_N = 1$, so that the first and last inputs are $x_1 = \tilde{x}_1 + 1$ and $x_N = \tilde{x}_{N-1}$. Also, as in the bipartite case, there is the convention that if the index $\tilde{x} > m$, it is replaced by $\tilde{x} - m$ and a term $+1$ is added to the sum. As an example, in the particular case $N = 3$ the above formulas simplify to

$$\begin{aligned} X_{\tilde{x}_1,\tilde{x}_2} &= A^{(1)}_{\tilde{x}_1} - A^{(2)}_{\tilde{x}_1+\tilde{x}_2-1} + A^{(3)}_{\tilde{x}_2}, \\ \overline{X}_{\tilde{x}_1,\tilde{x}_2} &= -A^{(1)}_{\tilde{x}_1+1} + A^{(2)}_{\tilde{x}_1+\tilde{x}_2-1} - A^{(3)}_{\tilde{x}_2}. \end{aligned} \tag{4.121}$$

Thus the expressions $P(X_{\tilde{x}_1,\tilde{x}_2}=k)$ are:

$$\begin{aligned} P(X_{\tilde{x}_1,\tilde{x}_2}=k) &= P(A^{(1)}_{\tilde{x}_1}-A^{(2)}_{\tilde{x}_1+\tilde{x}_2-1}+A^{(3)}_{\tilde{x}_2}=k) \\ &= \sum_{j_1,j_2=0}^{d-1} P(j_1,j_2,(k-j_1+j_2 \bmod d)|\tilde{x}_1,(\tilde{x}_1+\tilde{x}_2-1),\tilde{x}_2), \end{aligned} \tag{4.122}$$

following the same definition of equation (4.5) as in the bipartite case, which can be extended to N parties straightforwardly.

Optimal CGLMP measurements for more parties

The authors of [AGCA12] find that, in the limit of a high number of inputs $m \to \infty$, the maximal violation of their inequalities is attained by the generalised GHZ state $|\mathrm{GHZ}_{N,d}\rangle$ with the following optimal observables:

$$\begin{aligned} A^{(1)}_x &= U_x F_d \Omega_d F_d^\dagger U_x^\dagger, \\ A^{(2)}_x &= V_x F_d^\dagger \Omega_d F_d V_x^\dagger, \\ A^{(3)}_x &= W_x F_d \Omega_d F_d^\dagger W_x^\dagger \\ &\vdots \\ A^{(N-1)}_x &= \begin{cases} W_x F_d \Omega_d F_d^\dagger W_x^\dagger, & N \text{ even} \\ W_x^\dagger F_d^\dagger \Omega_d F_d W_x, & N \text{ odd} \end{cases} \\ A^{(N)}_x &= \begin{cases} W_x^\dagger F_d^\dagger \Omega_d F_d W_x, & N \text{ even} \\ W_x F_d \Omega_d F_d^\dagger W_x^\dagger, & N \text{ odd} \end{cases} \end{aligned} \tag{4.123}$$

with

$$F_d = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{ij} |i\rangle\langle j|, \qquad \Omega_d = \mathrm{diag}[1,\omega,\ldots,\omega^{d-1}] \tag{4.124}$$

and

$$U_x = \sum_{j=0}^{d-1} \omega^{-j\theta_U(x)} |j\rangle\langle j|, \qquad V_x = \sum_{j=0}^{d-1} \omega^{j\theta_V(x)} |j\rangle\langle j|, \qquad W_x = \sum_{j=0}^{d-1} \omega^{-j\theta_W(x)} |j\rangle\langle j|, \tag{4.125}$$

with $\theta_U(x) = (x-1/2)/m$, $\theta_V(x) = x/m$, and $\theta_W(x) = (x-1)/m$. Note that we have used directly the generalised observables notation introduced in Section 4.1. For the case $N = 2$ these measurements reproduce the optimal

CGLMP observables, so we will use them to construct the generalisation our Bell inequalities. Moreover, for these measurements and the state $|\mathrm{GHZ}_{\mathrm{N,d}}\rangle$, all the probabilities appearing in both $\mathbb{P}_k^N$ and $\mathbb{Q}_k^N$ are equal, that is,

$$P(X_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = k) = P(\overline{X}_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = k) \tag{4.126}$$

and

$$P(X_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = -k-1) = P(\overline{X}_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}} = -k-1) \tag{4.127}$$

for all sequences $\tilde{x}_1,\ldots,\tilde{x}_{N-1}$ with $\tilde{x}_i = 1,\ldots,m$. As in the bipartite case, this symmetry will be respected by the generic form of our Bell expressions.

Generalised correlators for many parties

Before going further, let us give the definition of the generalised correlators (4.10) for N parties, where (i) denotes the party:

$$\langle A_{x_1}^{(1)k_1}\ldots A_{x_N}^{(N)k_N}\rangle = \sum_{a_1\ldots a_N} \omega^{\boldsymbol{k}\cdot\boldsymbol{a}} P(a_1,\ldots,a_N|x_1,\ldots,x_N), \tag{4.128}$$

for $k_i = 0,\ldots,d-1$ $\forall i$, and where $\omega = \exp(2\pi\mathbb{i}/d)$ and $\boldsymbol{k}\cdot\boldsymbol{a} = a_1k_1+\cdots+a_Nk_N$. Recall from the bipartite case that one can think of $\{A_{x_i}^{(i)k_i}\}_{k_i}$ as an observable representation of a d-outcome measurement with outcomes labelled by $1,\omega,\ldots,\omega^{d-1}$; in particular, for quantum correlations, $A_{x_i}^{(i)k_i}$ are unitary operators with eigenvalues $1,\omega,\ldots,\omega^{d-1}$. The inverse transformation gives

$$P(a_1,\ldots,a_N|x_1,\ldots,x_N) = \frac{1}{d^N}\sum_{k_1\ldots k_N} \omega^{-(\boldsymbol{a}\cdot\boldsymbol{k})}\langle A_{x_1}^{(1)k_1}\ldots A_{x_N}^{(N)k_N}\rangle. \tag{4.129}$$

For 3 parties

For clarity, let us first present our construction in the case of three parties ($N=3$). We use the $\mathbb{P}_k^N$ and $\mathbb{Q}_k^N$ of Aolita *et al.* as the generalisation of the bipartite $\mathbb{P}_k$ and $\mathbb{Q}_k$ of equation (4.9). We thus start from the generic Bell expression:

$$I_{3,m,d} = \sum_{k=0}^{\lfloor d/2\rfloor-1}\left(\alpha_k\mathbb{P}_k^3 - \beta_k\mathbb{Q}_k^3\right), \tag{4.130}$$

where we recall that $\mathbb{P}_k^3$ and $\mathbb{Q}_k^3$ are given by

$$\begin{aligned}\mathbb{P}_k^3 &= \sum_{\tilde{x}_1,\tilde{x}_2=1}^{m}\left[P(A_{\tilde{x}_1}^{(1)} - A_{\tilde{x}_1+\tilde{x}_2-1}^{(2)} + A_{\tilde{x}_2}^{(3)} = k) + P(A_{\tilde{x}_1+\tilde{x}_2-1}^{(2)} - A_{\tilde{x}_1+1}^{(1)} - A_{\tilde{x}_2}^{(3)} = k)\right],\\ \mathbb{Q}_k^3 &= \sum_{\tilde{x}_1,\tilde{x}_2=1}^{m}\left[P(A_{\tilde{x}_1}^{(1)} - A_{\tilde{x}_1+\tilde{x}_2-1}^{(2)} + A_{\tilde{x}_2}^{(3)} = -k-1)\right.\\ &\qquad\left. + P(A_{\tilde{x}_1+\tilde{x}_2-1}^{(2)} - A_{\tilde{x}_1+1}^{(1)} - A_{\tilde{x}_2}^{(3)} = -k-1)\right],\end{aligned} \tag{4.131}$$

while α_k and β_k are our degrees of freedom. For instance, for $\alpha_k = \beta_k = [1 - 2k/(d-1)]$, (4.130) reproduces the Bell inequalities (4.117) of Aolita *et al.* We now want to exploit these degrees of freedom in order to obtain Bell inequalities maximally violated by $|\mathrm{GHZ}_{3,d}\rangle$. Let us use the generalised correlators (4.128) to rewrite the generic Bell expression:

$$\widetilde{I}_{3,m,d} = \sum_{\tilde{x}_1,\tilde{x}_2=1}^{m}\sum_{l=1}^{d-1}\langle \bar{A}_{\tilde{x}_1}^{(1)l}(A_{\tilde{x}_1+\tilde{x}_2-1}^{(2)})^{-l}A_{\tilde{x}_2}^{(3)l}\rangle, \tag{4.132}$$

where the new variables $\bar{A}_{\tilde{x}_1}^{(1)l}$ are defined as

$$\bar{A}_{\tilde{x}_1}^{(1)l} = a_l A_{\tilde{x}_1}^{(1)l} + a_l^* A_{\tilde{x}_1+1}^{(1)l} \tag{4.133}$$

with

$$a_l = \sum_{k=0}^{\lfloor d/2\rfloor-1}\left(\alpha_k\omega^{-lk} - \beta_k\omega^{l(k+1)}\right). \tag{4.134}$$

Note here that as, due to the definition, $A_{m+1}^{(1)l} = \omega^l A_1^{(1)l}$, and therefore in the case of $\tilde{x} = m$, equation (4.133) reads $\bar{A}_m^{(1)l} = a_l A_m^{(1)l} + a_l^*\omega^{-l}A_1^{(1)l}$. Let us also notice that the term in (4.132) corresponding to $l = 0$ is a constant and therefore it is not included in the new Bell expression $\widetilde{I}_{3,m,d}$, which we also rescaled by a factor d.

Now, to fix our free parameters α_k and β_k ($k = 0,\ldots,\lfloor d/2\rfloor - 1$) we require that for the optimal observables (4.123) the following conditions

$$\bar{A}_{\tilde{x}_1}^{(1)l} \otimes (A_{\tilde{x}_1+\tilde{x}_2-1}^{(2)})^{-l} \otimes A_{\tilde{x}_2}^{(3)l}|\mathrm{GHZ}_{3,d}\rangle = |\mathrm{GHZ}_{3,d}\rangle \tag{4.135}$$

are satisfied for all $\tilde{x}_1, \tilde{x}_2 = 1,\ldots,m$. In other words, we want to find such α_k and β_k that the resulting operator $\bar{A}_{\tilde{x}_1}^{(1)l} \otimes (A_{\tilde{x}_1+\tilde{x}_2-1}^{(2)})^{-l} \otimes A_{\tilde{x}_2}^{(3)l}$ stabilises the GHZ state, meaning that the GHZ state is its eigenstate with eigenvalue one. This condition is analogous to condition (4.21) of the bipartite case. To solve the above equations we need the explicit forms of the lth powers of the measurements (4.123). After some algebra one finds that

$$A_{\tilde{x}_1}^{(1)l} = \omega^{-(d-l)\theta_U(\tilde{x}_1)} \sum_{n=0}^{l-1} |d-l+n\rangle\langle n| + \omega^{l\theta_U(\tilde{x}_1)} \sum_{n=l}^{d-1} |n-l\rangle\langle n|, \tag{4.136}$$

$$(A_{\tilde{x}_2}^{(2)})^{-l} = (A_{\tilde{x}_2}^{(2)l})^{\dagger} = \omega^{(d-l)\theta_V(\tilde{x}_2)} \sum_{n=0}^{l-1} |d-l+n\rangle\langle n| + \omega^{-l\theta_V(\tilde{x}_2)} \sum_{n=l}^{d-1} |n-l\rangle\langle n|, \tag{4.137}$$

and

$$A_{\tilde{x}_3}^{(3)l} = \omega^{-(d-l)\theta_W(\tilde{x}_3)} \sum_{n=0}^{l-1} |d-l+n\rangle\langle n| + \omega^{l\theta_W(\tilde{x}_3)} \sum_{n=l}^{d-1} |n-l\rangle\langle n|. \tag{4.138}$$

By plugging (4.136), (4.137) and (4.138) into the conditions (4.135), one obtains the following system of linear equations for the coefficients a_l:

$$\begin{cases} a_l \omega^{-l/2m} + a_l^* \omega^{l/2m} = 1 \\ a_l \omega^{(l-k)/2m} + a_l^* \omega^{-(d-l)/2m} = 1 \end{cases} \tag{4.139}$$

with $l = 1, \ldots, \lfloor d/2 \rfloor$. This system can be directly solved, giving

$$a_l = \frac{\omega^{\frac{2l-d}{4m}}}{2\cos(\pi/2m)} \qquad (l = 1, \ldots, \lfloor d/2 \rfloor). \tag{4.140}$$

We have arrived to exactly the same system (4.32) as in the bipartite case. We can thus follow the same procedure and obtain the same coefficients

$$\alpha_k = \frac{1}{2d} \tan\left(\frac{\pi}{2m}\right) [g(k) - g(\lfloor d/2 \rfloor)] \tag{4.141}$$

$$\beta_k = \frac{1}{2d} \tan\left(\frac{\pi}{2m}\right) [g(k+1-1/m) + g(\lfloor d/2 \rfloor)] \tag{4.142}$$

valid for odd and even d, with $k = 1, \ldots, \lfloor d/2 \rfloor$ and $g(x) := \cot[\pi(x+1/2m)/d]$.

For any number of parties

Calculations for any number N of parties follow the same spirit. Our generic Bell expression becomes:

$$I_{N,m,d} = \sum_{k=0}^{\lfloor d/2 \rfloor} (\alpha_k \mathbb{P}_k^N - \beta_k \mathbb{Q}_k^N), \tag{4.143}$$

in which $\mathbb{P}_k^N$ and $\mathbb{Q}_k^N$ were defined in (4.118), following Aolita *et al.* As in the case of two and three parties, we can rewrite $I_{N,m,d}$ in terms of the complex correlators as

$$\widetilde{I}_{N,m,d} = \sum_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}=1}^{m} \sum_{l=1}^{d-1} \left\langle \prod_{i=1}^{N} (A^{(i)}_{\tilde{x}_{i-1}+\tilde{x}_i-1})^{(-1)^{i-1}l} \right\rangle, \tag{4.144}$$

where $\tilde{x}_0 = 1, \tilde{x}_N = 1$, and $A^{(1)}_{\tilde{x}_1} = \bar{A}^{(1)}_{\tilde{x}_1}$. The variables $\bar{A}^{(1)l}_{\tilde{x}_1}$ are, as before, combinations of $A^{(1)l}_{\tilde{x}_1}$ and $A^{(1)l}_{\tilde{x}_1+1}$ given by

$$\bar{A}^{(1)l}_{\tilde{x}_1} = a_l A^{(1)l}_{\tilde{x}_1} + a_l^* A^{(1)l}_{\tilde{x}_1+1} \tag{4.145}$$

with a_l defined as in (4.134). Notice that the term corresponding to $l = 0$ is only a constant that was removed from the new Bell expression $\widetilde{I}_{N,m,d}$, which we also rescaled by a factor of d.

The above form of the Bell expression suggests the conditions one needs to impose on the variables α_k and β_k in order to obtain a Bell inequality maximally violated by the N-partite GHZ state $|\mathrm{GHZ}_{N,d}\rangle$. As before, we want the operator appearing in the Bell expression to stabilise the GHZ state. Namely, the following system of equations

$$\bigotimes_{i=1}^{N} (A^{(i)}_{\tilde{x}_{i-1}+\tilde{x}_i-1})^{(-1)^{i-1}l} |\mathrm{GHZ}_{N,d}\rangle = |\mathrm{GHZ}_{N,d}\rangle, \tag{4.146}$$

with the same conventions as for (4.144), should hold for any choice of $\tilde{x}_i$ and l with the measurements being given in (4.123). We find the same system of equations for a_l as we obtained in the bipartite and tripartite case (4.139) with its solution given in (4.140). Thus, our Bell inequalities for any number of parties are determined through the same coefficients α_k and β_k as in the cases $N = 2, 3$. Note that to go from $I_{N,m,d}$ to $\widetilde{I}_{N,m,d}$ one can use:

$$\widetilde{I}_{N,m,d} = dI_{N,m,d} - 2m^{N-1}S, \tag{4.147}$$

where $S = \sum_k (\alpha_k - \beta_k)$ and is thus given by equation (4.44).

Conclusion

To conclude, for N parties, our Bell inequalities are given in probability form $I_{N,m,d}$ by equation (4.143) and in correlators form $\widetilde{I}_{N,m,d}$ by equation (4.144), with coefficients α_k (4.141) and β_k (4.142) being the same as in the bipartite case. To obtain them, we followed the approach of [AGCA12] to get the generalisation of the CGLMP measurements as well as a generic Bell expression. We then imposed that the GHZ state should be "stabilised" under our Bell expression, and proceeded from this condition as in the bipartite case.

4.2.2. Properties of the Bell expressions

Here we will characterise our class of Bell inequalities. We obtain analytically and prove the Svetlichny quantum, and no-signalling bounds, proving thereby that the maximal quantum violation is indeed attained with the state $|\mathrm{GHZ}_{N,d}\rangle$. The case of the classical bound is more complicated, so we leave it for last. We denote these bounds, respectively, $\widetilde{\beta}_S^{N,m,d}$, $\widetilde{\beta}_Q^{N,m,d}$, $\widetilde{\beta}_{NS}^{N,m,d}$, $\widetilde{\beta}_C^{N,m,d}$ for $\widetilde{I}_{N,m,d}$, and the ones for $I_{N,m,d}$ are denoted without the tilde, and can be obtained via equation (4.147).

Svetlichny bound

We start by considering a hybrid local-nonlocal model introduced in Section 2.2.4, which leads to a bound particular to the multipartite case where local correlations are shared inside any bipartition of the system, while between bipartition nonlocal correlations are allowed.

Theorem 4.8. *The Svetlichny bound of $\widetilde{I}_{N,m,d}$ is given by $\widetilde{\beta}_S^{N,m,d} = m^{N-2}\widetilde{\beta}_C^{2,m,d}$, where $\widetilde{\beta}_C^{2,m,d}$ is the classical bound of the Bell inequality in the bipartite case and is given by (4.78).*

Proof. Let us follow the same outline as in the proof of [AGCA12]. To this end, we decompose the variables in equations (4.119) and (4.120) as

$$X_{\tilde{\boldsymbol{x}}} = A_{\tilde{x}_1}^{(1)} - X'_{\tilde{x}_1,\tilde{\boldsymbol{x}}'}, \qquad \overline{X}_{\tilde{\boldsymbol{x}}} = -A_{\tilde{x}_1+1}^{(1)} + X'_{\tilde{x}_1,\tilde{\boldsymbol{x}}'}, \tag{4.148}$$

where $\tilde{\boldsymbol{x}}' = \tilde{x}_2, \ldots, \tilde{x}_{N-1}$. This isolates the first party $A^{(1)}$. With this notation, our Bell expression $I_{N,m,d}$ can be rewritten as

$$\sum_{k=0}^{\lfloor d/2\rfloor} (\alpha_k \mathbb{P}_k^N - \beta_k \mathbb{Q}_k^N) = \sum_{\tilde{\boldsymbol{x}}'} I_{2,m,d}^{\tilde{\boldsymbol{x}}'}, \tag{4.149}$$

where $I_{2,m,d}^{\tilde{\boldsymbol{x}}'}$ are bipartite Bell expression between the variables of the first party and joint variables involving the remaining parties

$$I_{2,m,d}^{\tilde{\boldsymbol{x}}'} = \\ \sum_{k=0}^{\lfloor d/2\rfloor}\sum_{\tilde{x}_1=1}^{m}\Big\{\alpha_k\Big[P(A_{\tilde{x}_1}^{(1)} - X_{\tilde{x}_1,\tilde{\boldsymbol{x}}'} = k) + P(-A_{\tilde{x}_1+1}^{(1)} + X_{\tilde{x}_1,\tilde{\boldsymbol{x}}'} = k)\Big] \\ -\beta_k\Big[P(A_{\tilde{x}_1}^{(1)} - X_{\tilde{x}_1,\tilde{\boldsymbol{x}}'} = -k-1) + P(-A_{\tilde{x}_1+1}^{(1)} + X_{\tilde{x}_1,\tilde{\boldsymbol{x}}'} = -k-1)\Big]\Big\}. \tag{4.150}$$

Each $I_{2,m,d}^{\tilde{\boldsymbol{x}}'}$ has the local bound $\beta_C^{2,m,d}$ and there are m^{N-2} terms in $\sum_{\tilde{\boldsymbol{x}}'} I_{2,m,d}^{\tilde{\boldsymbol{x}}'}$. Thus, for any correlations $\vec{p}$ which are bilocal with respect to the bipartition $A^{(1)}|A^{(2)}\dots A^{(N)}$, $I_{N,m,d} \leq m^{N-2}\beta_C^{2,m,d}$. One can then follow the argumentation of [AGCA12] which holds for our Bell expressions and use their symmetries to show that this remains valid for any bipartition. Thus, the Svetlichny bound of the Bell expression $I_{N,m,d}$ is $m^{N-2}\beta_C^{2,m,d}$, and the same relation is valid for $\widetilde{I}_{N,m,d}$ and $\widetilde{\beta}_C^{2,m,d}$. □

Let us notice that for the case $N = 3$ and $m = 2$ the bound $\widetilde{\beta}_S^{3,2,d}$ is also saturated by fully product probability distribution $P^{(1)}(a_1|x_1)P^{(2)}(a_2|x_2)P^{(3)}(a_3|x_3)$ such that $P^{(i)}(0|x_i) = 1$ for all x_i and i. So, in this case the Svetlichny and classical bound coincide. In general, however, this is not true.

Quantum bound

Theorem 4.9. *The quantum bound of $\widetilde{I}_{N,m,d}$ is $\widetilde{\beta}_Q^{N,m,d} = m^{N-1}(d-1)$.*

Proof. As in the bipartite case, we find an SOS decomposition of the shifted Bell operator $\widetilde{\beta}_Q^{N,m,d}\mathbb{I} - \mathcal{B}$. Let us start from the simpler case of $m = 2$ and introduce the following operators

$$P_{\tilde{x}_1,\dots,\tilde{x}_{N-1}}^{k} = \mathbb{I} - \bigotimes_{i=1}^{N}(A_{\tilde{x}_{i-1}+\tilde{x}_i-1}^{(i)})^{(-1)^{i-1}k}, \tag{4.151}$$

with the usual conventions $\tilde{x}_0 = 1, \tilde{x}_N = 1$, and $A_{\tilde{x}_1}^{(1)} = \bar{A}_{\tilde{x}_1}^{(1)}$. Then, the sum of squares in this case reads

$$\widetilde{\beta}_Q^{N,2,d}\mathbb{I} - \mathcal{B} = \frac{1}{2}\sum_{\tilde{x}_1,\dots,\tilde{x}_{N-1}=1}^{2}\sum_{k=1}^{d-1}\left(P_{\tilde{x}_1,\dots,\tilde{x}_{N-1}}^{k}\right)^{\dagger}P_{\tilde{x}_1,\dots,\tilde{x}_{N-1}}^{k}. \tag{4.152}$$

In the case of arbitrary number of measurements, the above sum of squares needs to be slightly modified. Introducing the following operators

$$T_x^k = \mu_{x,k}^* A_2^{(1)k} + \nu_{x,k}^* A_{x+2}^{(1)k} + \tau_{x,k} A_{x+3}^{(1)k} \tag{4.153}$$

for $x = 1, \ldots, m-2$ and $k = 1, \ldots, d-1$, where the coefficients are defined as

$$\begin{aligned}\mu_{x,k} &= \frac{\omega^{(x+1)(d-2k)/2m}}{2\cos(\pi/2m)} \frac{\sin(\pi/m)}{\sqrt{\sin(\pi x/m)\sin\left[\pi(x+1)/m\right]}},\\ \nu_{x,k} &= -\frac{\omega^{(d-2k)/2m}}{2\cos(\pi/2m)}\sqrt{\frac{\sin\left[\pi(x+1)/m\right]}{\sin(\pi x/m)}},\\ \tau_{x,k} &= \frac{1}{2\cos(\pi/2m)}\sqrt{\frac{\sin(\pi x/m)}{\sin\left[\pi(x+1)/m\right]}} = -\frac{\omega^{(d-2k)/2m}}{4\cos^2(\pi/2m)}\nu_{x,k}^{-1},\end{aligned} \tag{4.154}$$

for $i = 1, \ldots, m-3$ and $k = 1, \ldots, d-1$, while for $i = m-2$ and $k = 1, \ldots, d-1$ they are given by

$$\begin{aligned}\mu_{m-2,k} &= -\frac{\omega^{-(d-2k)/2m}}{2\sqrt{2}\cos(\pi/2m)\sqrt{\cos(\pi/m)}},\\ \nu_{m-2,k} &= -\frac{\omega^k \omega^{(d-2k)/2m}}{2\sqrt{2}\cos(\pi/2m)\sqrt{\cos(\pi/m)}},\\ \tau_{m-2,k} &= \frac{\sqrt{\cos(\pi/m)}}{\sqrt{2}\cos(\pi/2m)}.\end{aligned} \tag{4.155}$$

Then, the sum of square is given by

$$\widetilde{\beta}_Q^{N,m,d}\mathbb{I} - \mathcal{B} = \frac{1}{2}\sum_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}=1}^{m}\sum_{k=1}^{d-1}\left(P_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}}^k\right)^\dagger P_{\tilde{x}_1,\ldots,\tilde{x}_{N-1}}^k + \frac{m^{N-2}}{2}\sum_{x=1}^{m-2}\sum_{k=1}^{d-1}\left(T_x^k\right)^\dagger T_x^k. \tag{4.156}$$

To conclude the proof, let us notice that for the state $|\mathrm{GHZ}_{N,d}\rangle$ and the measurements (4.123) the value of $\widetilde{I}_{N,m,d}$ is $m^{N-1}(d-1)$, which follows from the fact that in this setting, every correlator under the sum equals one. The bound $\widetilde{\beta}_Q^{N,m,d}$ is thus tight. □

No-signalling bound

Theorem 4.10. *The no-signalling bound of $\widetilde{I}_{N,m,d}$ is given by $\widetilde{\beta}_{NS}^{N,m,d} = m^{N-2}\widetilde{\beta}_{NS}^{2,m,d}$, where $\widetilde{\beta}_{NS}^{2,m,d}$ is the no-signalling bound of the Bell inequality in the bipartite case and is given by (4.104).*

Proof. We proceed as in the proof of the bipartite case. Let us start with our Bell expression in the probability form $I_{N,m,d}$ and rewrite it as

$$I_{N,m,d} = \sum_{k=0}^{d-1} \alpha_k \mathbb{P}_k^N, \tag{4.157}$$

where $\mathbb{P}_k^N$ is given in equation (4.118) and $\alpha_k = -\beta_{d-1-k}$ for $k = \lfloor d/2 \rfloor, \ldots, d-1$ (notice that in the odd d case $\alpha_{\lfloor d/2 \rfloor} = \beta_{\lfloor d/2 \rfloor} = 0$). As shown Section 4.1.2, the coefficients are such that $\alpha_0 \geq \alpha_k$ for any $0 \leq k \leq d-1$. The algebraic bound of $I_{N,m,d}$ clearly follows, as it corresponds to putting all the terms in $\mathbb{P}_0^N$ equal to 1:

$$I_{N,m,d} \leq 2m^{N-1}\alpha_0. \tag{4.158}$$

The algebraic bound is also the no-signalling bound, as there exists a no-signalling probability distribution for which this inequality is saturated. We now give this distribution. For the following measurement choices, it is defined as

$$\begin{aligned} &P(a_1, \ldots, a_N | \tilde{x}_1, \tilde{x}_1 + \tilde{x}_2 - 1, \ldots, \tilde{x}_{N-2} + \tilde{x}_{N-1} - 1, \tilde{x}_{N-1}) \\ &\qquad = \begin{cases} \dfrac{1}{d^{N-1}}, & \text{when } \displaystyle\sum_{i=1}^{N} (-1)^{i-1} a_i = f(\tilde{x}_1, \ldots, \tilde{x}_{N-1}) \\ 0, & \text{otherwise} \end{cases}, \end{aligned} \tag{4.159}$$

where whenever $\tilde{x}_{i-1} + \tilde{x}_i - 1 > m$ for some $i = 2, \ldots, N-1$ it is replaced by $\tilde{x}_{i-1} + \tilde{x}_i - 1 - m$, and the function f is defined as

$$f(\tilde{x}_1, \ldots, \tilde{x}_{N-1}) = \sum_{i=1}^{N-2} (-1)^{i+1} H(\tilde{x}_{i-1} + \tilde{x}_i - m - 2). \tag{4.160}$$

Here, H is the discrete Heaviside step function, defined as $H(x) = 1$ if $x \geq 0$ and $H(x) = 0$ otherwise. This function f is introduced to take into account the definition $A_{m+k}^{(j)} = A_k^{(j)} + 1$, which modifies the condition defining the probabilities in the Bell expression when the measurement index goes over m. Indeed, looking at the expression (4.118), one sees that if for all $i = 1, \ldots, N-2$, $\tilde{x}_i + \tilde{x}_{i+1} - 1 \leq m$, then $f = 0$, but if for some j's, $\tilde{x}_j + \tilde{x}_{j+1} - 1 > m$, then f could be different than 0. In the same way one has, for the following measurement choices:

$$P(a_1,\ldots,a_N|\tilde{x}_1+1,\tilde{x}_1+\tilde{x}_2-1,\ldots,\tilde{x}_{N-2}+\tilde{x}_{N-1}-1,\tilde{x}_{N-1}) \\ = \begin{cases} \frac{1}{d^{N-1}}, & \sum_{i=1}^{N}(-1)^{i-1}a_i = \widetilde{f}(\tilde{x}_1,\ldots,\tilde{x}_{N-1}) \\ 0, & \text{otherwise} \end{cases}, \tag{4.161}$$

where, if $\tilde{x}_1+1>m$ or $\tilde{x}_{i-1}+\tilde{x}_i-1>m$ for some $i=2,\ldots,N-1$ we replace it by, respectively, $\tilde{x}_1+1-m$ or $\tilde{x}_{i-1}+\tilde{x}_i-1-m$, and the function $\widetilde{f}$ is defined in the same way as f, but also takes into account that $\tilde{x}_1+1$ can be larger than m. Thus

$$\widetilde{f}(\tilde{x}_1,\ldots,\tilde{x}_{N-1}) = -H(\tilde{x}_1-m)+f(\tilde{x}_1,\ldots,\tilde{x}_{N-1}). \tag{4.162}$$

For all the remaining choices of measurements we assume the distribution

$$P(a_1,\ldots,a_N|x_1\ldots x_N) = \frac{1}{d^N}. \tag{4.163}$$

Let us now recall the no-signalling principle for many parties. For the distribution of elements $P(a_1,\cdots,a_N|x_1\cdots x_N)$, the marginal $P(a_{i_1},\cdots,a_{i_k}|x_{i_1},\cdots,x_{i_k})$ for any subset $\{i_1,\cdots,i_k\}$ of the N parties should be independent of the measurement settings of the remaining $N-k$ parties:

$$P(a_{i_1},\cdots,a_{i_k}|x_1,\cdots,x_N) = P(a_{i_1},\cdots,a_{i_k}|x_{i_1},\cdots,x_{i_k}). \tag{4.164}$$

One can verify that the distribution presented above obeys the no-signalling principle. Tracing out a single subsystem one always obtains a maximally random probability distribution. Thus, since the bipartite no-signalling bound of $I_{2,m,d}$ was $\beta_{NS}^{2,m,d}=2m\alpha_0$, we have that $\beta_{NS}^{N,m,d}=m^{N-2}\beta_{NS}^{2,m,d}$, and this relation remains valid for $\widetilde{I}_{N,m,d}$ and $\widetilde{\beta}_{NS}^{N,m,d}$. □

Classical bound

Let us start with our Bell expression in probability form, rewritten as in equation (4.157)

$$I_{N,m,d} = \sum_{k=0}^{d-1}\alpha_k\mathbb{P}_k^N, \tag{4.165}$$

where, we recall:

$$\mathbb{P}_k^N = \sum_{\tilde{\boldsymbol{x}}}\left[P(X_{\tilde{\boldsymbol{x}}}=k)+P(\overline{X}_{\tilde{\boldsymbol{x}}}=k)\right]. \tag{4.166}$$

As in the bipartite case, we want to find the best deterministic strategy, i.e. distribute 0s and 1s so as to have the highest value of $I_{N,m,d}$. This means assigning variables that we denote q and r to combinations of variables $X_{\tilde{\boldsymbol{x}}} = q(\tilde{\boldsymbol{x}})$ and $\overline{X}_{\tilde{\boldsymbol{x}}} = r(\tilde{\boldsymbol{x}})$. The optimisation is then done over these variables q, r:

$$\max I_{N,m,d} = \max_{q,r} \sum_{k=0}^{d-1} \alpha_k \sum_{\tilde{\boldsymbol{x}}} (\delta(q(\tilde{\boldsymbol{x}}), k) + \delta(r(\tilde{\boldsymbol{x}}), k)), \tag{4.167}$$

where δ is the Dirac delta. This is what we had done in the bipartite case in equation (4.80), with a slightly different notation. In the bipartite case, these variables had to obey a superselection rule (4.81) (i.e. we had removed linear dependencies between the variables). The problem of removing the linear dependencies means finding $s, g(x), h(x)$ such that

$$s + \sum_{x=1}^{m} [g(x)q(x) + h(x)r(x)] = 0 \mod d. \tag{4.168}$$

In the current notation, rule (4.81) then reads:

$$\sum_{x=1}^{m} [q(x) + r(x)] \equiv -1 \mod d. \tag{4.169}$$

For N parties, finding this rule is not so straightforward. The problem we have to solve is to find all $s, g(\tilde{\boldsymbol{x}}), h(\tilde{\boldsymbol{x}}) \in \mathbb{Z}^d$ such that

$$s + \sum_{\tilde{\boldsymbol{x}}} [g(\tilde{\boldsymbol{x}})q(\tilde{\boldsymbol{x}}) + h(\tilde{\boldsymbol{x}})r(\tilde{\boldsymbol{x}})] \equiv 0 \mod d. \tag{4.170}$$

We note that the above equation can be expanded as

$$s + \sum_{j=1}^{N} \sum_{\tilde{\boldsymbol{x}}} \left[g(\tilde{\boldsymbol{x}})(-1)^{j-1} A^{(j)}_{\tilde{x}_{j-1}+\tilde{x}_j-1} + h(\tilde{\boldsymbol{x}})(-1)^j A^{(j)}_{\tilde{x}'_{j-1}+\tilde{x}'_j-1} \right] \equiv 0 \mod d, \tag{4.171}$$

where we recall that $\tilde{x}_0 = \tilde{x}_N = 1$ but $\tilde{x}'_0 = 2$ and $\tilde{x}'_N = 1$ (see (4.119) and (4.120)), hence the $\tilde{x}'_i$ notation. We observe that $\tilde{x}_{j-1} + \tilde{x}_j - 1 = \tilde{x}'_{j-1} + \tilde{x}'_j - 1$ if $1 < j < N$, and that for $j = N$ we get $\tilde{x}_{j-1} + \tilde{x}_j - 1 = \tilde{x}'_{j-1} + \tilde{x}'_j - 1 = \tilde{x}_{N-1}$. Therefore, this gives the set of equations that make the coefficient in front of $A^{(N)}_{\tilde{x}_{N-1}}$ congruent to $0 \mod d$:

$$\sum_{\tilde{\boldsymbol{x}}:\tilde{x}_{N-1}=k} [g(\tilde{\boldsymbol{x}}) - h(\tilde{\boldsymbol{x}})] \equiv 0 \mod d, \qquad 1 \leq k \leq m. \tag{4.172}$$

Similarly, for $1 < j < N$, we make the coefficient in front of $A_k^{(j)}$ congruent to $0 \mod d$:

$$\sum_{\tilde{\boldsymbol{x}}:\tilde{x}_{j-1}=k+1-\tilde{x}_j} [g(\tilde{\boldsymbol{x}}) - h(\tilde{\boldsymbol{x}})] \equiv 0 \mod d, \qquad 1 \leq k \leq m. \tag{4.173}$$

For the case $j = 1$ we note that $\tilde{x}_0 + \tilde{x}_1 - 1 = \tilde{x}_1$ and $\tilde{x}'_0 + \tilde{x}'_1 - 1 = \tilde{x}_1 + 1$. Hence, the coefficient that accompanies $A_{\tilde{x}_1}^{(1)}$ is

$$\sum_{\tilde{\boldsymbol{x}}:\tilde{x}_1=k} [g(k;\tilde{x}_2\ldots\tilde{x}_{N-1}) - h(k-1;\tilde{x}_2\ldots\tilde{x}_{N-1})] \equiv 0 \mod d, \qquad 1 \leq k \leq m. \tag{4.174}$$

Finally, we have an equation for the constant term. Here we have to take into consideration that $A_{m+k}^{(j)} = A_k^{(j)} + 1$ if $k > 0$. Note also that we only need to consider $k < m$ because of the form of the inequality. Let us denote by $C_{\tilde{\boldsymbol{x}},j}, C'_{\tilde{\boldsymbol{x}},j} \in \{0,1\}$ the constant picked by exceeding the value of m in the measurement settings: $A_{\tilde{x}_{j-1}+\tilde{x}_j-1}^{(j)} = A_{\tilde{x}_{j-1}+\tilde{x}_j-1 \mod' m}^{(j)} + C_{\tilde{\boldsymbol{x}},j}$ and $A_{\tilde{x}'_{j-1}+\tilde{x}'_j-1}^{(j)} = A_{\tilde{x}'_{j-1}+\tilde{x}'_j-1 \mod' m}^{(j)} + C'_{\tilde{\boldsymbol{x}},j}$, where $\mod'$ means that the modulo is taken from 1 to m instead of 0 to $m-1$.

$$a + \sum_{j=1}^{N} \sum_{\tilde{\boldsymbol{x}}} (-1)^{j+1} [g(\tilde{\boldsymbol{x}}) C_{\tilde{\boldsymbol{x}},j} - h(\tilde{\boldsymbol{x}}) C'_{\tilde{\boldsymbol{x}},j}] \equiv 0 \mod d \tag{4.175}$$

Note that $C_{\tilde{\boldsymbol{x}},j} = C'_{\tilde{\boldsymbol{x}},j}$ if $j > 1$, which, combined to the above equations leads to

$$a + \sum_{\tilde{\boldsymbol{x}}} (g(\tilde{\boldsymbol{x}}) C_{\tilde{\boldsymbol{x}},1} - h(\tilde{\boldsymbol{x}}) C'_{\tilde{\boldsymbol{x}},1}) + \sum_{\tilde{\boldsymbol{x}}} (g(\tilde{\boldsymbol{x}}) - h(\tilde{\boldsymbol{x}})) \sum_{j=2}^{N} C_{\tilde{\boldsymbol{x}},j} (-1)^{j+1} \equiv 0 \mod d \tag{4.176}$$

The conditions we just derived can be used to solve the optimisation problem of the classical bound for a few cases, which we did with Mathematica [Wol14]. A few analytical values are presented in Table A.3, and a comparison of the numerical values for the Svetlichny and the classical bounds for a few cases is reported in Table A.4 (all tables can be found in Appendix A). We leave the general case as an open question.

4.2.3. Discussion

In this section, we generalised our bipartite inequalities to any number of parties N and studied the bounds of the resulting inequalities. Proving the Tsirelson bound meant finding a generalisation of our SOS to many parties. Let us note the important point that the bounds of $I_{N,m,d}$ are all related to the bounds of $I_{2,m,d}$ by the factor m^{N-2} (the Svetlichny bound being related to the bipartite classical bound by this factor). We became aware that the authors of [BBB$^+$12] found that, if one generalises a Bell inequality to more parties by following the procedure of [AGCA12] as we did, this relation between the bounds would hold (more precisely, they showed it for the Tsirelson bound and the Svetlichny bound). One can thus apply directly the results of [BBB$^+$12] to get an alternative proof of the Theorems 4.8 and 4.9 above. This relation between the bounds means that the results about their relative scaling from Section 4.1.2 also hold for many parties. As an open question, it would be interesting to see whether a general expression could be found for the classical bound, valid for any N, m, d.

4.3. A class of Bell inequalities for partially entangled states

Let us recall the generic bipartite Bell expressions of equation (4.8):

$$I_{m,d} = \sum_{k=0}^{\lfloor d/2 \rfloor -1} \left(\alpha_k \mathbb{P}_k - \beta_k \mathbb{Q}_k \right),$$

and recall that this expression yields our inequalities for some specific values of the coefficients α_k, β_k, while it yields the CGLMP/BKP inequalities for other values of those coefficients. Knowing that these different Bell inequalities are maximally violated by different entangled states, it is natural to ask whether we could find a general relation between coefficients α_k, β_k and the corresponding optimal state. We first answer this question in the particular case of two parties, two inputs and three outputs.

4.3.1. The Bell expressions

For $N = 2$, $m = 2$ and $d = 3$, (4.8) gives a class of Bell inequalities involving two parameters $\alpha_0 \mathbb{P}_0 - \beta_0 \mathbb{Q}_0 \leq \beta_C$. However, we can always divide the whole expression by one of them, say α_0 (provided that it is positive), reducing the number of free parameters to one. As a result we obtain the following class of Bell inequalities

$$J_{2,2,3}(\xi) = P(A_1 = B_1) + P(A_2 = B_2) + P(A_1 = B_2 - 1) + P(A_2 = B_1)$$

$$- \xi[P(A_1 = B_1 - 1) + P(A_2 = B_2 - 1) + P(A_1 = B_2) + P(A_2 = B_1 + 1)] \tag{4.177}$$

parametrised by a single parameter which we denote ξ and which is defined in terms of the coefficients as $\xi = \beta_0/\alpha_0$. It turns out that the classical bound of these inequalities can be found by looking for the local deterministic strategy that maximises $J_{2,2,3}(\xi)$:

$$\beta_C^{2,2,3}(\xi) = \begin{cases} -4\xi, & \text{if } \xi \leq -1, \\ 3 - \xi, & \text{if } -1 \leq \xi \leq 1, \\ 2, & \text{if } \xi \geq 1. \end{cases} \tag{4.178}$$

Moreover, numerical tests using the NPA hierarchy (see Section 2.2.3) indicate that for $\xi \leq -1$, the Bell inequality (4.177) is trivial, meaning that its maximal quantum violation equals its classical bound. Consequently, in what follows we will concentrate on the case $\xi > -1$. It is then not difficult to see that for $\xi = 1$ the class (4.177) reproduces the well-known CGLMP Bell inequality, which is known to be maximally violated by the partially entangled state [ADGL02]:

$$|\psi_\gamma\rangle = \frac{1}{\sqrt{2+\gamma^2}}(|00\rangle + \gamma|11\rangle + |22\rangle) \tag{4.179}$$

with $\gamma = (\sqrt{11} - \sqrt{3})/2$, whereas for $\xi = (\sqrt{3} - 1)/2$ it gives our Bell inequality $I_{2,3}$ from Section 4.1. In both cases the optimal CGLMP observables are used to get the maximal quantum violation.

The question we want to answer now is whether by changing ξ between the above two values we can obtain Bell inequalities maximally violated by partially entangled states (4.179) for various values of γ. To answer this question let us first take the optimal CGLMP measurements and the state $|\psi_\gamma\rangle$ and compute the value of the Bell expression (4.177). This gives us the following function of ξ and γ:

$$\mathcal{J}(\xi, \gamma) = \frac{4[3 + \gamma(2\sqrt{3} + \gamma - \xi\gamma)]}{3(2+\gamma^2)}. \tag{4.180}$$

To find its maximal value for a fixed ξ, we need to satisfy the following condition $\partial\mathcal{J}(\xi,\gamma)/\partial\gamma = 0$. Solving this equation is equivalent to finding the root of a second degree polynomial in γ, and the extremum is found to be

$$\gamma_+(\xi) = [(4\xi^2 + 4\xi + 25)^{1/2} - 2\xi - 1]/2\sqrt{3}, \tag{4.181}$$

for which the maximal value of (4.180) for a fixed ξ is

$$\mathcal{J}_{\max}(\xi) = \frac{1}{3}\left[5 - 2\xi + \sqrt{25 + 4(\xi+1)\xi}\right]. \tag{4.182}$$

Of course, the above derivation is not a proof that this is the quantum bound of the Bell expression (4.177), however, based on our numerical study we conjecture this to be the case. Notice first that for $\xi = 1$ and $\xi = (\sqrt{3}-1)/2$, the expression (4.182) reproduces the maximal quantum violations of the CGLMP and of our Bell inequalities. Then, we tested our conjecture numerically for other values of ξ by using the NPA hierarchy (see Section 2.2.3 for details). We employed this technique for values of $\xi \in [-0.99, 100]$ with the step 0.01, and for all these values of ξ the value obtained agrees with (4.182) up to solver precision 10^{-8}, which is a strong implication that it is the maximal quantum violation of the corresponding inequality. Note that for $\xi \in [-0.99, 42]$, the level $1 + AB$ of the hierarchy was sufficient, while for $\xi \in [42, 100]$ we used the level 2, except for a small amount of values in the interval $[85, 100]$ for which the level $2 + AAB$ was necessary. To conclude, let us also write the class of inequalities (4.177) in the correlator form

$$\begin{aligned} J_{2,2,3}(\xi) &= a(\xi)\langle A_1B_1\rangle + a^*(\xi)\omega\langle A_1B_2\rangle + a(\xi)\langle A_2B_2\rangle + a^*(\xi)\langle A_2B_1\rangle + \text{c.c.} \\ &= 2\text{Re}\left[\langle A_1\bar{B}_1\rangle + \langle A_2\bar{B}_2\rangle\right] \end{aligned} \tag{4.183}$$

where $a(\xi) = 1 - \xi\omega$ with $\omega = \exp(2\pi\mathbb{i}/3)$, , and $\bar{B}_1 = a(\xi)B_1 + a^*(\xi)\omega B_2$ and $\bar{B}_2 = a(\xi)B_2 + a^*(\xi)B_1$.

4.3.2. Extension to more parties

The extension of the last section to more parties turns out to be straightforward, and we study it for $N = 3$ and $N = 4$. We follow the same procedure: we start from the N-partite version of (4.8), expression (4.143) and divide it by one the parameters so that there is only one that remains:

$$J_{3,2,3}(\xi) = \mathbb{P}_0^{(3)} - \xi\mathbb{Q}_0^{(3)}, \tag{4.184}$$

$$J_{4,2,3}(\xi) = \mathbb{P}_0^{(4)} - \xi\mathbb{Q}_0^{(4)}. \tag{4.185}$$

We can perform an optimisation to conjecture the classical bound of these inequalities:

$$\beta_C^{3,2,3}(\xi) = \begin{cases} -8\xi, & \text{if } \xi \leq -1, \\ 2(3-\xi), & \text{if } -1 \leq \xi \leq 1, \\ 4, & \text{if } \xi \geq 1. \end{cases} \tag{4.186}$$

$$\beta_C^{4,2,3}(\xi) = \begin{cases} -16\xi, & \text{if } \xi \leq -10/11, \\ 10-5\xi, & \text{if } -10/11 \leq \xi \leq 2/5, \\ 8, & \text{if } \xi \geq 2/5. \end{cases} \tag{4.187}$$

Let us now consider the following states, partially entangled GHZ states:

$$|\mathrm{GHZ}_\gamma^{(3)}\rangle = \frac{1}{\sqrt{2+\gamma^2}}(|000\rangle + \gamma|111\rangle + |222\rangle), \tag{4.188}$$

$$|\mathrm{GHZ}_\gamma^{(4)}\rangle = \frac{1}{\sqrt{2+\gamma^2}}(|0000\rangle + \gamma|1111\rangle + |2222\rangle). \tag{4.189}$$

As in the section above, we compute the values $\mathcal{J}^{(3)}(\xi,\gamma)$ and $\mathcal{J}^{(4)}(\xi,\gamma)$ of the Bell expressions for the corresponding partially entangled GHZ states and the CGLMP measurements (4.123), then find the value of $\gamma(\xi)$ by solving $\partial\mathcal{J}(\xi,\gamma)/\partial\gamma = 0$. We obtain that:

$$\gamma^{(3)}(\xi) = \gamma^{(4)}(\xi) = \frac{\sqrt{4\xi^2+4\xi+25} - 2\xi - 1}{2\sqrt{3}}, \tag{4.190}$$

which is the same value as for $N = 2$. Entering (4.190) into the values of the Bell expressions, we get:

$$\mathcal{J}_{\max}^{(3)}(\xi) = 2(1 + 2\xi + \sqrt{25 + 4(\xi+1)\xi}), \tag{4.191}$$

$$\mathcal{J}_{\max}^{(4)}(\xi) = 4(1 + 2\xi + \sqrt{25 + 4(\xi+1)\xi}). \tag{4.192}$$

We conjecture that (4.191) and (4.192) are the maximal quantum violations of $J_{3,2,3}(\xi)$ and $J_{4,2,3}(\xi)$, respectively. To support this conjecture, we use the NPA hierarchy as above. With the change of scenario, it takes significantly more time to solve each SDP, so we do not check as many values of ξ as in the section above. For $N = 3$, we checked values of $\xi \in [-1, 5]$ with step 0.1 and found that the values agreed up to 10^{-7} or lower. For $N = 4$, we checked values of $\xi \in [-1, 2]$ with step 0.5 and found that the values agreed up to 10^{-8} or lower.

4.3.3. Open questions

We conjectured that the class of Bell inequalities $J_{2,2,3}(\xi)$ is maximally violated by a class of partially entangled states $|\psi_{\gamma(\xi)}\rangle$ with the parameter γ a function of ξ. Results of this kind could be very useful in experiments: imagine for instance a setup where a specific state $|\psi_\gamma\rangle$ is the easiest to produce – the most adequate Bell inequality $J_{2,2,3}(\xi(\gamma))$ could then be chosen to analyse the results. We generalised our conjecture to three and four parties. Note that we also studied but did not include here the case of $J_{2,2,4}(\xi)$. We were able to find some results, but the mathematical expressions became complicated and the numerical evidence less straightforward. It would be interesting to see whether our conjectures could be proven analytically, perhaps by finding an SOS decomposition for $J_{2,2,3}(\xi)$, which might then shed light on higher dimensional cases.

4.4. Experimental realisation

A team of researchers from the Technical University of Denmark and the University of Bristol, UK, recently developed a quantum device based on integrated photonics, a “quantum chip”. This device is able to generate multidimensional entanglement as well as to manipulate and measure it, fully on-chip. The generated qudits are path-encoded, by having each photon exist over d spatial modes simultaneously, and entanglement is produced by a coherent and controllable excitation of an array of d identical photon-pair sources. The device is able to generate and manipulate entangled states of two photons of local dimension up to 15. Projective measurements can be performed, as universal operations on path-encoded qudits are possible in linear-optics for any dimension.

This device was used to demonstrate quantum processing applications, in particular high-dimensional ones which were not experimentally explored before. Among these applications, violations of the CGLMP inequalities and of our inequalities were measured, leading to self-testing and randomness expansion for some values of d. We first present the experimental setup in more details, and we then explain our contribution to the study. Note that several concepts in the description of the setup were not covered in Chapter 2 – we thus refer the reader to [GK04, OPSV13] if needed.

4.4.1. The setup

Entangled path-encoded qubits can be generated by coherently pumping two spontaneous parametric down conversion [SPL+12, COP+16] or spontaneous four-wave mixing (SFWM) photon-pair sources [SBO+13, WBV+16]. The approach can be generalized to qudits via the generation of photons entangled over d spatial modes by coherently pumping d sources [SPL+12, KHLZ17]. However, scaling this approach to high dimensions has represented a significant challenge, due to the need of a stable and scalable technology able to coherently embed large arrays of identical photon sources and to precisely control qudit states in large optical interferometers.

Silicon quantum photonics, offering intrinsic stability [SBO+13, BST16], high precision [WPS+17, PGS+17] and dense integration [HSP+17, STY+13], can provide a natural solution. A large-scale silicon quantum photonic circuit was devised to implement the scheme, as shown in Figure 4.3 and Figure 4.4. A total of 16 SFWM sources are coherently pumped, generating a photon-pair in a superposition across the array. As both the photons must originate from the same source, the bipartite state created is $\sum_{k=0}^{d-1} c_k |1\rangle_{i,k} |1\rangle_{s,k}$ where $|1\rangle_{i,k}$ ($|1\rangle_{s,k}$) indicates the Fock state of the idler (signal) photon being in its k-th

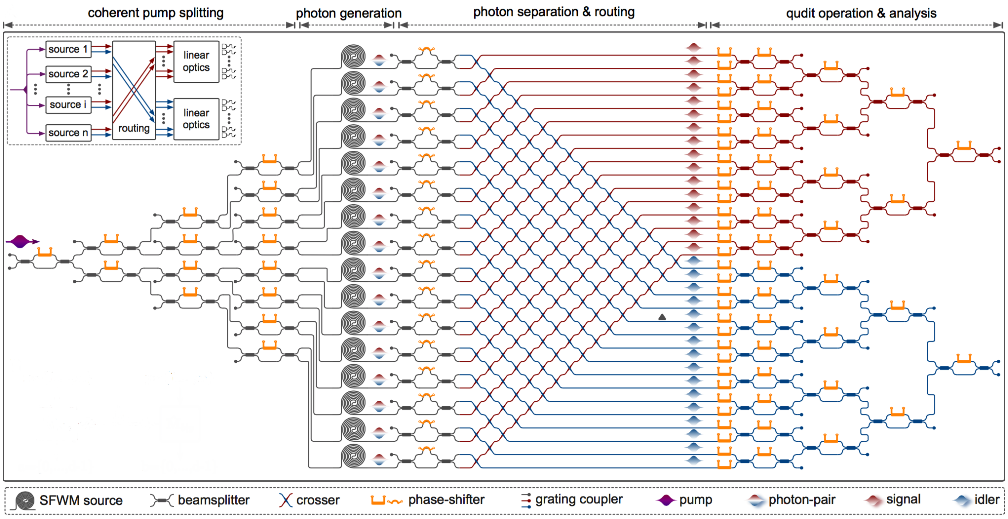

Figure 4.3.: Circuit diagram. The device monolithically integrates 16 SFWM photon-pair sources, 93 thermo-optical phase-shifters, 122 multimode interferometers (MMI) beamsplitter, 256 waveguide-crossers and 64 optical grating couplers. A photon pair is generated by SFWM in superposition across 16 optical modes, producing a tunable multidimensional bipartite entangled state. The two photons, signal and idler, are separated by an array of asymmetric MZI filters and routed by a network of crossers, allowing the local manipulation of the state by linear-optical circuits. Using triangular networks of MZIs, arbitrary local projective measurements are performed. The inset represents a general schematic for universal generation and manipulation of bipartite multidimensional entangled states.

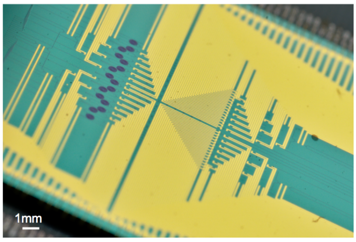

Figure 4.4.: Photograph of the device. Silicon waveguides and 16 SFWM sources can be observed as black lines. Gold wires allow the electronic access of each phase-shifter.

spatial mode and c_k represents the complex amplitude in each mode (with $\sum |c_k|^2 = 1$). The mapping between the Fock state of each photon and the logical state is the following: we say that the qudit state is $|k\rangle$ ($k = 0, \ldots, d-1$) if the associated photon is in its k-th optical mode. This yields an arbitrary multidimensional entangled state:

$$|\psi_d\rangle = \sum_{k=0}^{d-1} c_k |k\rangle_i |k\rangle_s, \tag{4.193}$$

where the coefficients c_k can be arbitrarily chosen by controlling the pump distribution over the d sources and the relative phase on each mode. This is achieved using a network of Mach-Zehnder interferometers (MZIs) at the input and phase-shifters on each mode, as shown in Figure 4.3. In particular, maximally entangled states $|\phi_d^+\rangle = \sum_{k=0}^{d-1} |k\rangle_i |k\rangle_s / \sqrt{d}$ can be obtained with a uniform excitation of the sources. The two non-degenerate photons are deterministically separated using asymmetric MZI filters and routed by a network of waveguide crossings, grouping the signal photon into the top modes and the idler photon into the bottom ones (see Figure 4.3). The state of each qudit can then be locally manipulated and measured. Linear-optical circuits enable the implementation of any local unitary transformation $\hat{U}_d$ in dimension d [RZBB94, CHM+16, CHS+15]. Here a triangular network of MZIs and phase-shifters are used, as shown in Figure 4.3, which allows arbitrary local projective measurements to be performed.

The 16 photon-pair sources are designed to be identical. Two-photon reversed Hong-Ou-Mandel (RHOM) interference is used to verify their performance, where the fringe visibility gives an estimate of the sources' indistinguishability [SBO+13]. RHOM interference is tested between all the possible pairs of the 16 sources, performing $\binom{16}{2} = 120$ quantum interference experiments and evaluating the corresponding visibilities. The pair of sources used for each interference experiment is selected each time by reconfiguring the interferometric network. Approximately a 2kHz photon-pair detection rate is observed in typical measurement conditions. In Figure 4.5 the measured visibilities are reported. In all cases, a visibility of at least 0.90 was obtained, and more than 80% cases presented at least 0.98 visibility. These results show a state-of-the-art degree of source indistinguishability in all 120 RHOM experiments, leading to the generation of high quality entangled qudit states.

Each of the MZIs and phase-shifters can be rapidly reconfigured (kHz rate) with high precision [BST16, HSP+17]. The quality of the qudit projectors is characterised by the classical statistical fidelity, which quantifies the output distribution obtained preparing and measuring a qudit on a fixed basis. As re-

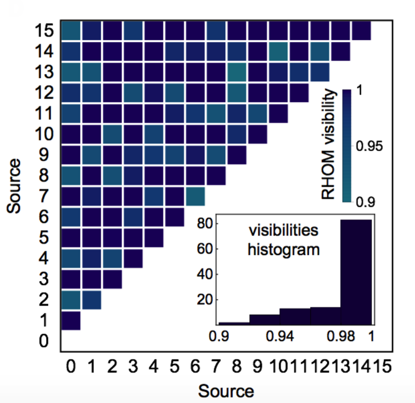

Figure 4.5.: Visibilities for the two-photon RHOM experiments to test sources' indistinguishability. The inset shows the histogram of all 120 measured visibilities, with a mean value of 0.984 ± 0.025.

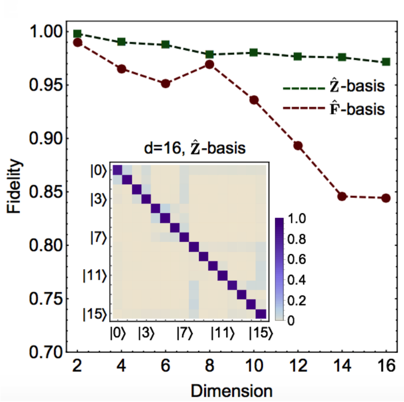

Figure 4.6.: Statistical fidelity for d-dimensional projectors, in both the computational $\hat{Z}$-basis and the Fourier $\hat{F}$-basis. The inset shows the measured distribution for the 16-dimensional projector in the $\hat{Z}$-basis.

ported in Figure 4.6, the fidelity of projectors was measured in dimension $d = 2$ to 16 in both the computational basis $\hat{Z} = |k\rangle\langle k|$, and in the Fourier-transform basis $\hat{F} = |\ell\rangle\langle\ell|$, where $|\ell\rangle = \sum_{k=0}^{d-1} e^{2\pi i k\ell/d}|k\rangle/\sqrt{d}$ and $k, \ell = 0, \ldots, d-1$. For $d = 8$ fidelities of 98% are observed in the $\hat{Z}$-basis and 97% in the $\hat{F}$-basis, while for $d = 16$ fidelities of 97% in the $\hat{Z}$-basis and 85% in the $\hat{F}$-basis. The residual imperfections are mainly due to thermal cross-talk between phase-shifters (higher in the $\hat{F}$-basis), which can be mitigated using optimised designs for the heaters [HSP+17] or ad-hoc characterisation techniques [CHS+15, PGS+17].

Due to a fabrication imperfection in the routing circuit one of the modes (triangle label in Figure 4.3) for the idler photon presents an additional 10 dB loss. For simplicity this lossy mode is excluded in the experiment, so we study multidimensional entanglement for dimension up to 15.

4.4.2. Experimental values for our inequalities and applications

The setup presented above was used to measure violations of the CGLMP inequalities as well as our Bell inequalities (4.17) for 2 inputs i.e. $\widetilde{I}_{2,2,d}$, that we denote:

$$\widetilde{I}_d = \sum_{i=1}^{2}\sum_{l=1}^{d-1}\langle A_i^l \bar{B}_i^l\rangle, \tag{4.194}$$

for $d = 2, \ldots, 8$. The maximally entangled state of dimension d and the optimal CGLMP measurements of Section 4.1.1 were used in both cases. The observed values are reported in Table A.5 (all Tables can be found in Appendix A). For both Bell inequalities and for all d considered, the classical bound is violated. In particular for our inequalities, in dimensions 2–4 a strong violation is observed, closely approaching the Tsirelson bound. Also for CGLMP, strong violations of LHV models are observed (it is not expected to closely approach the Tsirelson bound, as the state is not optimal for CGLMP).

For more details, the experimental values of the generalised correlators $\mathrm{Re}[\langle A_i^l \bar{B}_i^l\rangle]$ that enter into the computation of the values of our Bell inequalities are presented in Figure 4.7. Figure 4.8 plots the values of $\tilde{I}_d$ from Table A.5, together with the quantum and classical bounds.

Self-testing

Let us use these observed values along with the SWAP method (which was presented in Section 2.3.4) to perform self-testing. Recall that it was shown in [YVB+14] that the state maximally violating CGLMP, $|\psi_\gamma\rangle$ with $\gamma = (\sqrt{11} - \sqrt{3})/2$ could be self-tested using this method. Also, we've shown in Section 4.1.3 that the maximally entangled state of two qutrits could be self-tested

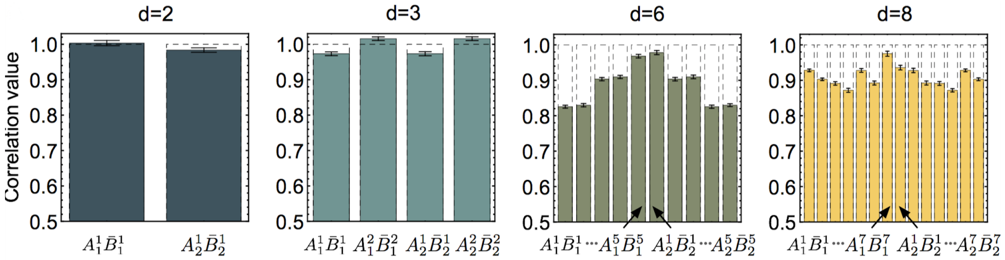

Figure 4.7.: Measured values of the $2(d-1)$ correlators $\mathrm{Re}[\langle A_i^l \bar{B}_i^l \rangle]$ from expression $\widetilde{I}_d$. Dashed boxes refers to theoretical values and errors are estimated from photon Poissonian statistics.

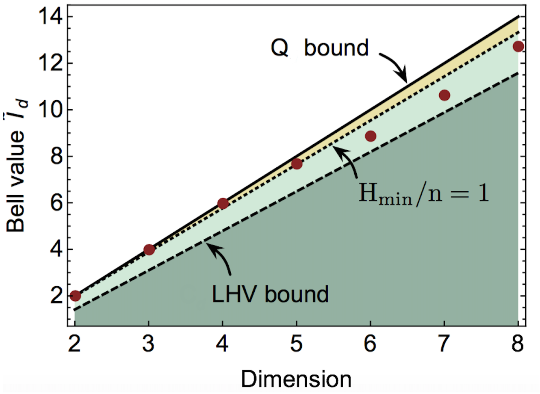

Figure 4.8.: The red points are experimentally measured values of $\widetilde{I}_d$. The dashed line corresponds to the classical (or LHV) bound β_C, and the solid line is the Tsirelson bound β_Q. The dotted line represents the threshold above which more than 1 global random bit can be certified.

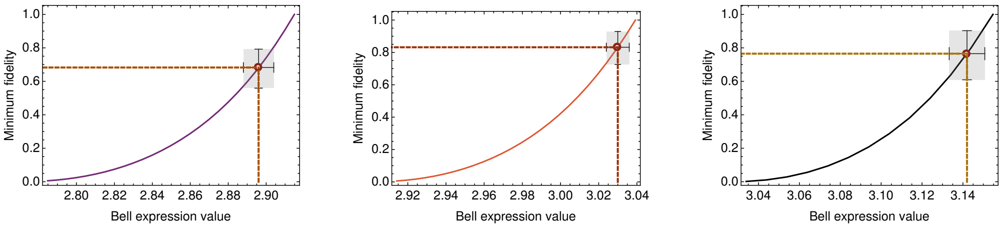

Figure 4.9.: Minimum fidelity between the physical state and the reference state $|\psi_\gamma\rangle$ for three values of γ, as a function of the violation of the corresponding Bell expression $J_{2,2,3}(\xi)$ (which includes CGLMP and $\widetilde{I}_3$). From left to right, $\gamma = 0.7923$, $\gamma = 0.9$ and $\gamma = 1$. At the maximal violation, the fidelity is equal to 1, meaning that the quantum state used in the Bell experiment must be equal to the reference state. For lower violations, the fidelity decreases. The self-tested fidelities for the violations measured experimentally are depicted as points in the figure, with error bars estimated from photon Poissonian statistics.

from the maximal violation of $\widetilde{I}_3$. Here we applied this method to another state of the class $|\psi_\gamma\rangle$, with the value $\gamma = 0.9$. For this, we used the Bell inequality $J_{2,2,3}(\xi)$ for partially entangled states presented in Section 4.3. This indicates that more states of the form $|\psi_\gamma\rangle$ might be self-tested using their corresponding $J_{2,2,3}(\xi)$. All three fidelity curves are represented in Figure 4.9.

We then used measured violations of CGLMP, $\widetilde{I}_3$, and $J_{2,2,3}(\xi)$ to compute corresponding experimental self-testing fidelities. These violations were obtained by performing optimal CGLMP measurements on the $|\psi_\gamma\rangle$ with adequate γ. Complete results with robustness are displayed in Figure 4.9, as well as in Tables A.6 and A.7. To conclude, we remark that the certification of high fidelities in a self-testing context is only achievable in the presence of near-ideal experimental correlations – here, the measured self-tested fidelities are comparable with the reported values obtained from full tomographies in other experimental approaches [ALM+11, KRR+17].

Randomness expansion

We also study the randomness that can be certified with our experimental observations. We consider the global randomness (using both Alice and Bob's outputs). Let us note that it is a particularly demanding task to generate randomness efficiently – to generate more than 1 bit of randomness per output

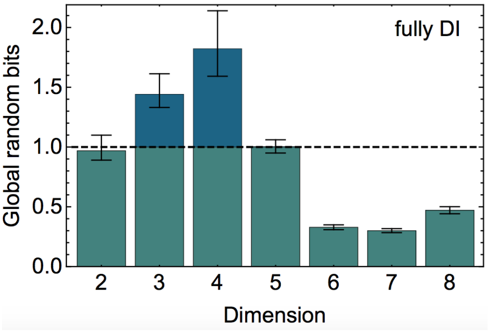

Figure 4.10.: Global randomness $H_{\min}^{x,y}$ certified per round, based on the observed violation of $\widetilde{I}_d$ (see Table A.5) for different values of d. Above the dashed line more than 1 private random bits are generated. Error bars are given by Poissonian statistics.

symbol, i.e. to achieve $H_{\min}^{x,y} > n$ with n the number of rounds. In that regime randomness expansion is naturally achieved as more than one private random bit is obtained per round. We saw in Section 2.3.2 that this was only possible for qubits using special scenarios with non-projective measurements [APVW16] or with sequences of measurements [CJA$^+$17]. In contrast, multidimensional entangled states provide a natural route to certify more randomness, based on projective measurements, where up to $n \log_2 d$ bit of randomness can be expected in the ideal case. The necessary Bell inequality violation so that $H_{\min}^{x,y} > n$ is pictured in Figure 4.8.

Our results are presented in Figure 4.10 and Table A.8. Note that we take the worst-case min-entropy among the different pairs of inputs. The largest amount of randomness is obtained for $d = 4$, where $H_{\min}^{x,y} = 1.82 \pm 0.35$ random bits. The amount of certified randomness is low for higher dimensions, since the fully device-independent framework is sensitive to noise.

4.5. Discussion

In this chapter, we introduced Bell expressions valid for any number m of measurement choices and any number d of measurement outcomes that are maximally violated by the maximally entangled states. We studied their properties and applied a numerical method to self-test the maximally entangled state of two qutrits. We then presented a generalisation of the Bell expressions to any number of parties which are maximally violated by generalised GHZ states. We also studied a class of Bell inequalities for three outcomes which covers our

Bell expressions as well as the CGLMP ones, and whose quantum bound, we conjecture, is attained by a class of partially entagled states of two qutrits. Finally, we presented our experimental collaboration where violations of our Bell expressions were observed which allowed for state self-testing and randomness expansion in a few scenarios.

Several questions remain open, and perhaps the main one concerns self-testing: can we prove it in other scenarios, perhaps for any number of outputs, and further, for any number of inputs and any number of parties? Also, can we find an analytical proof that the Bell inequalities $J_{2,2,3}(\xi)$ are indeed maximally violated by states $|\psi_{\gamma(\xi)}\rangle$, and perhaps a generalisation to a higher number of outputs? More generally, can we use elements of our method to derive other Bell inequalities with desirable quantum properties? It would also be interesting to study the DIQKD properties of our Bell inequalities further.

5. Randomness from partially entangled states

The device-independent approach does not exclude considerations about the states and measurements in a Bell test, even though the results are independent of those states and measurements. For instance, one can take an entangled state and wonder: how much randomness can be certified from this state? Or: which measurements should be applied onto this state to produce correlations which will guarantee a maximal amount of randomness? In this context, entanglement can be seen as a *resource* to produce randomness, which, of course, remains certified by the correlations only.

In [AMP12], the authors showed that 1 bit of local randomness could be certified from any partially entangled state of two qubits:

$$|\psi_\theta\rangle = \cos(\theta/2)|00\rangle + \sin(\theta/2)|11\rangle, \tag{5.1}$$

where $\theta \in]0, \pi/2]$. The certification was based on the maximal violation of I_β, a tilted CHSH expression they introduced. When considering global randomness however, they only proved that when $\theta \to 0$, arbitrarily close to 2 bits of randomness could be certified. This last state is almost separable. On the other side of the entanglement scale, we know that 2 bits of global randomness can be certified from the maximally entangled state $|\phi^+\rangle$, as discussed in Chapter 3. What about all the states in between those extremes?

In this chapter, we answer this question and show how 2 bits of global randomness can be certified from any partially entangled state of two qubits, i.e. any $\theta \in]0, \pi/2]$. We first present an approach based on a combination of two I_β and one CHSH expression. We also prove that, when considering POVMs, 2 bits of local randomness can be certified from these states. We then present a second approach where we introduce a modification of the Elegant Bell inequality [Gis09], for which we find an SOS decomposition as well as a self-testing procedure in the ideal case. This approach requires less measurement inputs than the first one, but is only valid for a certain range of entangled states.

5.1. An approach based on the tilted CHSH inequality

Let us start with our first approach which is valid for any state $|\psi_\theta\rangle$ with $0 < \theta \leq \pi/2$. We first present the scenario, in which Alice and Bob observe the maximal violation of two tilted CHSH inequalities I_β, and a non-maximal violation of a CHSH inequality. We then show how these conditions guarantee (or self-test) a certain form of the measurements of Alice and Bob as well as the state, and how randomness certification (both global and local) ensues.

5.1.1. Scenario and intuition

Let us write the density operator $\psi_\theta = |\psi_\theta\rangle\langle\psi_\theta|$ associated to $|\psi_\theta\rangle$ as

$$\psi_\theta = \frac{1}{4}\Big[\mathbb{I}\otimes\mathbb{I} + \cos(\theta)\big(\mathbb{I}\otimes Z + Z\otimes\mathbb{I}\big) + \sin(\theta)\big(X\otimes X - Y\otimes Y\big) + Z\otimes Z\Big] \tag{5.2}$$

This notation allows us to get some intuition on how to proceed. Indeed, Alice and Bob will need to do measurements in the X-Y plane of the Bloch sphere in order to generate the two bits of randomness, as the symmetry in the Z direction is broken, compared to the case of the maximally entangled state (putting $\theta = \pi/2$ in (5.2)). On the other hand, there will be a tendency for the maximum of a Bell inequality to be attained with at least some of the measurements having a component along the Z axis since the terms involving Z are larger in magnitude than those involving X and Y. Thus, we look for a scheme that involves measurements spanning *all three dimensions* of the Bloch sphere.

In the scheme we consider here, Alice performs three measurements A_1, A_2, A_3 and Bob performs seven measurements $B_1, \ldots, B_7$ on a state that is a priori unknown but intended to be $|\psi_\theta\rangle$ in some basis for some $\theta \in]0, \frac{\pi}{2}]$. They check that the correlations they obtain satisfy the conditions

$$I_\beta = 2\sqrt{2}\sqrt{1+\beta^2/4}\,, \tag{5.3}$$

$$J_\beta = 2\sqrt{2}\sqrt{1+\beta^2/4}\,, \tag{5.4}$$

$$I_{\text{CHSH}} = 2\sqrt{2}\sin(\theta)\,, \tag{5.5}$$

$$\langle A_3B_7\rangle = -\sin(\theta)\,, \tag{5.6}$$

where

$$I_\beta = \beta\langle A_1\rangle + \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle\,, \tag{5.7}$$

$$J_\beta = \beta\langle A_1\rangle + \langle A_1B_3\rangle + \langle A_1B_4\rangle + \langle A_3B_3\rangle - \langle A_3B_4\rangle. \tag{5.8}$$

are tilted CHSH expressions of the kind introduced in [AMP12], more precisely they correspond to I_β^α with $\alpha = 1$. We set:

$$\beta = \frac{2\cos(\theta)}{\sqrt{1+\sin(\theta)^2}} \,. \tag{5.9}$$

The third Bell expression

$$I_{CHSH} = \langle A_2 B_5 \rangle + \langle A_2 B_6 \rangle + \langle A_3 B_5 \rangle - \langle A_3 B_6 \rangle \tag{5.10}$$

is an ordinary CHSH expression.

The idea of our proof is the following: the maximal violation of the tilted CHSH expressions I_β and J_β implies that $A_1 = Z$ (up to local isometries), and that A_2 and A_3 are on the X-Y plane of the Bloch sphere. Then, the violation of the CHSH expression $I_{CHSH} = 2\sqrt{2}\sin(\theta)$ requires A_2 and A_3 to be orthogonal on the Bloch sphere, i.e. $A_2 = X$ and $A_3 = Y$. The final condition $\langle A_3 B_7 \rangle = -\sin(\theta)$ requires that $B_7 = Y$. Then, the randomness can be certified by Alice and Bob performing their measurements $A_2 = X$ and $B_7 = Y$. Bob's other measurements $B_1, \cdots B_6$ are combinations of X and Z. What we just described is our reference experiment, and in the remainder of this chapter we will prove the equivalence with the physical experiment given conditions (5.3) – (5.6).

5.1.2. Self-test based on I_β

We now study how conditions (5.3) and (5.4) imply a certain form of the state and measurements used to obtain them. This is in fact a self-testing statement – note however that we do not introduce an explicit isometry. Let us rewrite the tilted CHSH expression introduced in [AMP12] as:

$$I_\beta = \beta\langle A \rangle + \langle AB \rangle + \langle AB' \rangle + \langle A'B \rangle - \langle A'B' \rangle \,, \tag{5.11}$$

with measurement operators A, A' for Alice, and B, B' for Bob acting on Hilbert spaces $\mathcal{H}_\mathrm{A}$ and $\mathcal{H}_\mathrm{B}$. For $0 \leq \beta < 2$, I_β satisfies the quantum bound

$$I_\beta \leq 2\sqrt{2}\sqrt{1+\beta^2/4} \tag{5.12}$$

which is strictly higher than the local bound $I_\beta \leq |\beta| + 2$. The quantum bound is tight and can be attained if Alice and Bob measure

$$A = Z \,, \qquad\qquad A' = X \tag{5.13}$$

and

$$B = \cos\left(\tfrac{\mu_\beta}{2}\right) Z + \sin\left(\tfrac{\mu_\beta}{2}\right) X \,, \tag{5.14}$$

$$B' = \cos\left(\tfrac{\mu_\beta}{2}\right) Z - \sin\left(\tfrac{\mu_\beta}{2}\right) X \tag{5.15}$$

on the two-qubit pure state

$$|\psi_\beta\rangle = \cos\left(\tfrac{\theta_\beta}{2}\right)|00\rangle + \sin\left(\tfrac{\theta_\beta}{2}\right)|11\rangle \,, \tag{5.16}$$

where μ_β and θ_β are related to β by

$$\sin(\theta_\beta) = \sqrt{\frac{1-\beta^2/4}{1+\beta^2/4}} \,, \qquad \cos(\theta_\beta) = \sqrt{\frac{2\,\beta^2/4}{1+\beta^2/4}} \,, \tag{5.17}$$

$$\sin\left(\tfrac{\mu_\beta}{2}\right) = \sqrt{\frac{1-\beta^2/4}{2}} \,, \qquad \cos\left(\tfrac{\mu_\beta}{2}\right) = \sqrt{\frac{1+\beta^2/4}{2}} \,. \tag{5.18}$$

Inversely, β and μ_β are related to θ_β by

$$\beta = \frac{2\cos(\theta_\beta)}{\sqrt{1+\sin(\theta_\beta)^2}} \,, \qquad \tan\left(\tfrac{\mu_\beta}{2}\right) = \sin(\theta_\beta) \,. \tag{5.19}$$

This tells us what value of β to choose and what measurements to do on Bob's side if we're aiming to identify a state for some given angle θ_β.

We have the following:

Lemma 5.1. *If the maximal quantum violation $\beta_Q = 2\sqrt{2}\sqrt{1+\beta^2/4}$ of I_β is observed, then there exists a choice of local basis in which the physical state has the form*

$$\rho = \psi_\beta \otimes \sigma_{\text{junk}} \,, \tag{5.20}$$

where $\psi_\beta = |\psi_\beta\rangle\langle\psi_\beta|$ is the pure qubit state of equation (5.16), σ_{junk} is the "junk" state, and Alice's measurements are

$$A = Z \otimes \mathbb{I} \,\oplus\, A_\perp \,, \tag{5.21}$$

$$A' = X \otimes \mathbb{I} \,\oplus\, A'_\perp \,, \tag{5.22}$$

where $Z \otimes \mathbb{I}$ and $X \otimes \mathbb{I}$ act only on the support of the marginal state $\rho_{\text{A}} = \text{Tr}_{\text{B}}[\rho]$ on Alice's side and $A_\perp$ and $A'_\perp$ act only on its orthogonal complement in Alice's Hilbert space $\mathcal{H}_{\text{A}}$.

The result is relatively straightforward, given the derivation of the quantum upper bound for the more general family of I_α^β expressions done in [AMP12]. We prove it in details for the special case I_β in Appendix B, in order to make our claims precise. Note also that a self-testing procedure was provided for I_β in [BP15].

5.1.3. Global randomness certification

We are now able to prove our main result:

Theorem 5.2. *In a Bell test where Alice makes three dichotomic measurements and Bob makes seven dichotomic measurements, if conditions* (5.3)–(5.6) *are satisfied, then the global guessing probability for inputs $x^* = 2, y^* = 7$ is bounded by:*

$$P_{guess}^{2,7} \leq 1/4. \tag{5.23}$$

This means that two bits of global randomness are certified.

Proof. From Lemma 5.1 and Appendix B, we know that if the first condition (5.3) is met, we can infer that, in a suitable choice of basis, the underlying quantum state has the form

$$\rho = \psi_\theta \otimes \sigma_{\text{junk}}, \tag{5.24}$$

and that the measurements A_1 and A_2 on Alice's side are

$$A_1 = Z \otimes \mathbb{I}\,, \tag{5.25}$$
$$A_2 = X \otimes \mathbb{I}\,. \tag{5.26}$$

Note that here and in the rest of the derivation, we restrict our attention to the part of the Hilbert space containing ρ, i.e., we take Alice's and Bob's marginals ρ_{A} and ρ_{B} to be of full rank. The second condition (5.4), i.e. $J_\beta = 2\sqrt{2}\sqrt{1+\beta^2/4}$ allows us to make an analogous claim for the state and measurements A_1 and A_3. However, we have already chosen a specific basis for our claims (5.24) – (5.26), which means that we cannot express A_3 as we wish. We will show that A_3 has the form $A_3 = Y \otimes A_Y$. What we know from the self-test is that A_3 must be related to A_1 by

$$\{A_1, A_3\} = 0 \tag{5.27}$$

regardless of the choice of basis. If we write:

$$A_3 = \mathbb{I} \otimes A_{\mathbb{I}} + X \otimes A_X + Y \otimes A_Y + Z \otimes A_Z\,, \tag{5.28}$$

imposing then (5.27) with $A_1 = Z \otimes \mathbb{I}$ forces $A_{\mathbb{I}} = A_Z = 0$. Requiring in addition that ${A_3}^2 = \mathbb{I} \otimes \mathbb{I}$, we find that the measurement A_3 must have the form

$$A_3 = X \otimes A_X + Y \otimes A_Y \tag{5.29}$$

with

$$A_X{}^2 + A_Y{}^2 = \mathbb{I}\,, \tag{5.30}$$

$$[A_X,\, A_Y] = 0\,. \tag{5.31}$$

We now study the third condition (5.5), i.e. $I_{CHSH} = 2\sqrt{2}\sin(\theta)$, and show that it implies $A_X = 0$. Writing

$$B_i = \mathbb{I}\otimes B_{\mathbb{I}}^{(i)} + X\otimes B_X^{(i)} + Y\otimes B_Y^{(i)} + Z\otimes B_Z^{(i)}\,, \tag{5.32}$$

with $i\in\{5,6\}$ for the measurements in I_{CHSH} on Bob's side, the condition $B_i{}^2 = \mathbb{I}\otimes\mathbb{I}$ implies that

$$B_{\mathbb{I}}^{(i)}{}^2 + B_X^{(i)}{}^2 + B_Y^{(i)}{}^2 + B_Z^{(i)}{}^2 = \mathbb{I}\,. \tag{5.33}$$

Note that, for the part in the X-Y plane, (5.33) implies

$$B_X^{(i)}{}^2 + B_Y^{(i)}{}^2 \leq \mathbb{I}\,. \tag{5.34}$$

Let us express I_{CHSH} with this notation. Using the expression (5.2) for ψ_θ in the Pauli basis and the fact that the Pauli operators are traceless, we get

$$\begin{aligned}\langle A_3B_5\rangle &= \mathrm{Tr}\big[A_3B_5\,(\psi_\theta\otimes\sigma_{\text{junk}})\big]\\ &= \sin(\theta)\big(\langle A_X\otimes B_X^{(5)}\rangle_{\text{junk}} - \langle A_Y\otimes B_Y^{(5)}\rangle_{\text{junk}}\big)\end{aligned} \tag{5.35}$$

and, similarly,

$$\langle A_3B_6\rangle = \sin(\theta)\,\big(\langle A_X\otimes B_X^{(6)}\rangle - \langle A_Y\otimes B_Y^{(6)}\rangle\big)\,, \tag{5.36}$$

$$\langle A_2B_5\rangle = \sin(\theta)\,\langle\mathbb{I}\otimes B_X^{(5)}\rangle\,, \tag{5.37}$$

$$\langle A_2B_6\rangle = \sin(\theta)\,\langle\mathbb{I}\otimes B_X^{(6)}\rangle\,. \tag{5.38}$$

The condition $I_{CHSH} = 2\sqrt{2}\sin(\theta)$ thus translates to

$$\langle\mathbb{I}\otimes B_X^{(5)}\rangle + \langle\mathbb{I}\otimes B_X^{(6)}\rangle + \langle A_X\otimes B_X^{(5)}\rangle - \langle A_Y\otimes B_Y^{(5)}\rangle - \langle A_X\otimes B_X^{(6)}\rangle + \langle A_Y\otimes B_Y^{(6)}\rangle = 2\sqrt{2} \tag{5.39}$$

Since $\mathbb{I}, A_X$ and A_Y commute, we can co-diagonalise them. Using also that $A_X{}^2 + A_Y{}^2 = \mathbb{I}$, we write

$$\mathbb{I} = \sum_k |k\rangle\langle k|\,, \tag{5.40}$$

$$A_X = \sum_k x_k|k\rangle\langle k|\,, \qquad A_Y = \sum_k y_k|k\rangle\langle k| \tag{5.41}$$

with ${x_k}^2 + {y_k}^2 = 1$, $\forall k$. Using this we have, for example,

$$\begin{aligned}\langle A_X \otimes B_X^{(5)} \rangle &= \sum_k x_k \operatorname{Tr}\big[\big(|k\rangle\langle k| \otimes B_X^{(5)}\big)\sigma_{\text{junk}}\big] \\ &= \sum_k x_k \langle B_X^{(5)} \rangle_k \end{aligned} \tag{5.42}$$

and similar expressions for the other terms on the left side of (5.39), where the expectation values $\langle \,\cdot\, \rangle_k = \operatorname{Tr}[\,\cdot\,\sigma_k]$ are evaluated on the states

$$\sigma_k = \operatorname{Tr}_{\mathrm{A}_{\text{junk}}}\big[\big(|k\rangle\langle k| \otimes \mathbb{I}\big)\sigma_{\text{junk}}\big] \tag{5.43}$$

on the "junk" part of the Hilbert space on Bob's side. Note that their norms satisfy

$$\sum_k \|\sigma_k\|^2 = \sum_k \operatorname{Tr}[\sigma_k] = 1\,. \tag{5.44}$$

Using this followed by a few applications of the Cauchy-Schwarz inequality to the left side of (5.39) gives

$$\begin{aligned}&\langle \mathbb{I} \otimes B_X^{(5)} \rangle + \langle \mathbb{I} \otimes B_X^{(6)} \rangle + \langle A_X \otimes B_X^{(5)} \rangle - \langle A_Y \otimes B_Y^{(5)} \rangle - \langle A_X \otimes B_X^{(6)} \rangle + \langle A_Y \otimes B_Y^{(6)} \rangle \\ &= \sum_k \Big[(1 + x_k)\langle B_X^{(5)} \rangle_k - y_k \langle B_Y^{(5)} \rangle_k + (1 - x_k)\langle B_X^{(6)} \rangle_k + y_k \langle B_Y^{(6)} \rangle_k\Big] \\ &\leq \sum_k \bigg(\sqrt{2(1 + x_k)}\sqrt{{\langle B_X^{(5)} \rangle_k}^2 + {\langle B_Y^{(5)} \rangle_k}^2} + \sqrt{2(1 - x_k)}\sqrt{{\langle B_X^{(6)} \rangle_k}^2 + {\langle B_Y^{(6)} \rangle_k}^2}\bigg) \\ &\leq \sum_k \Big(\sqrt{2(1 + x_k)}\, \|\sigma_k\|^2 + \sqrt{2(1 - x_k)}\, \|\sigma_k\|^2\Big) \\ &\leq \sum_k 2\sqrt{2}\, \|\sigma_k\|^2 \\ &= 2\sqrt{2}, \end{aligned} \tag{5.45}$$

where we used that ${x_k}^2 + {y_k}^2 = 1$ to get to the third expression and that $\langle B \rangle_k \leq \sqrt{\langle B^2 \rangle_k}\, \|\sigma_k\|$ and

$$\big\langle {B_X^{(i)}}^2 + {B_Y^{(i)}}^2 \big\rangle_k \leq \langle \mathbb{I} \rangle_k = \|\sigma_k\|^2 \tag{5.46}$$

to get to the fourth. Finally, the condition that (5.39) holds implies that all the inequalities used to get to the last line of (5.45) are actually equalities. In particular, the vectors $\big(\sqrt{2(1 + x_k)}, \sqrt{2(1 - x_k)}\big)$ and $\big(\|\sigma_k\|^2, \|\sigma_k\|^2\big)$ in the last application of the Cauchy-Schwarz inequality are collinear, which is only possible if $x_k = 0$ for all k. In other words, $A_X = 0$, and we conclude that Alice's third measurement must be of the form

$$A_3 = Y \otimes A_Y \tag{5.47}$$

with ${A_Y}^2 = \mathbb{I}$.

Finally, we apply the last condition $\langle A_3 B_7 \rangle = -\sin(\theta)$ to show that the probabilities of the possible outcomes when Alice and Bob jointly measure A_2 and B_7 are all 1/4. This amounts to showing that $\langle A_2 \rangle = \langle B_7 \rangle = \langle A_2 B_7 \rangle = 0$. Using the form $\rho = \psi_\theta \otimes \sigma_{\text{junk}}$ of the state and (5.2) for ψ_θ in the Pauli basis, for $A_2 = X \otimes \mathbb{I}$ we quickly obtain that $\langle A_2 \rangle = 0$. For the terms involving B_7, we can write B_7 as we did for B_5 and B_6 and obtain the same properties as in (5.34), i.e.,

$$B_7 = \mathbb{I} \otimes B_{\mathbb{I}}^{(7)} + X \otimes B_X^{(7)} + Y \otimes B_Y^{(7)} + Z \otimes B_Z^{(7)} \tag{5.48}$$

with

$${B_{\mathbb{I}}^{(7)}}^2 + {B_X^{(7)}}^2 + {B_Y^{(7)}}^2 + {B_Z^{(7)}}^2 = \mathbb{I}\,. \tag{5.49}$$

Let us compute $|\langle A_3 B_7 \rangle|$:

$$\begin{aligned} |\langle A_3 B_7 \rangle| &= \left| \langle Y \otimes Y \rangle_{\psi_\theta} \langle A_Y \otimes B_Y^{(7)} \rangle_{\text{junk}} \right| \\ &= |\sin(\theta)| \left| \langle A_Y \otimes B_Y^{(7)} \rangle \right| \\ &\leq |\sin(\theta)| \sqrt{\langle {B_Y^{(7)}}^2 \rangle} \sqrt{\langle {A_Y}^2 \rangle} \\ &= |\sin(\theta)| \sqrt{\langle B_Y^{(7)\,2} \rangle}\,. \end{aligned} \tag{5.50}$$

Applying now the condition $\langle A_3 B_7 \rangle = -\sin(\theta)$, we conclude that $\left\langle {B_Y^{(7)}}^2 \right\rangle = 1$. It follows from (5.49) that $\left\langle {B_{\mathbb{I}}^{(7)}}^2 \right\rangle = \left\langle {B_X^{(7)}}^2 \right\rangle = \left\langle {B_Z^{(7)}}^2 \right\rangle = 0$. This allows us to compute $\langle B_7 \rangle$ and $\langle A_2 B_7 \rangle$.

$$\begin{aligned} |\langle B_7 \rangle| &= \left| \langle \mathbb{I} \otimes \mathbb{I} \rangle_{\psi_\theta} \langle \mathbb{I} \otimes B_{\mathbb{I}}^{(7)} \rangle_{\text{junk}} + \langle \mathbb{I} \otimes Z \rangle_{\psi_\theta} \langle \mathbb{I} \otimes B_Z^{(7)} \rangle_{\text{junk}} \right| \\ &\leq \left| \langle \mathbb{I} \otimes B_{\mathbb{I}}^{(7)} \rangle \right| + \cos(\theta) \left| \langle \mathbb{I} \otimes B_Z^{(7)} \rangle \right| \\ &\leq \sqrt{\left\langle {B_{\mathbb{I}}^{(7)}}^2 \right\rangle} + \cos(\theta) \sqrt{\left\langle {B_Z^{(7)}}^2 \right\rangle} \\ &= 0\,. \end{aligned} \tag{5.51}$$

Moreover,

$$\begin{aligned}
|\langle A_2 B_7\rangle| &= \big|\langle X\otimes X\rangle_{\psi_\theta}\langle \mathbb{I}\otimes B_X^{(7)}\rangle_{\text{junk}}\big| \\
&= \sin(\theta)\big|\langle \mathbb{I}\otimes B_X^{(7)}\rangle\big| \\
&\leq \sin(\theta)\sqrt{\langle {B_X^{(7)}}^2\rangle} \\
&= 0\,.
\end{aligned} \tag{5.52}$$

We thus find, for all quantum realisations compatible with the four conditions (5.3)–(5.6) stated at the beginning, that

$$P(ab|27) \leq \frac{1}{4}\Big(1+|\langle A_2\rangle|+|\langle B_7\rangle|+|\langle A_2B_7\rangle|\Big) = \frac{1}{4}\,, \tag{5.53}$$

for $a,b\in\{0,1\}$, which means that $P_{\text{guess}}^{2,7}\leq 1/4$, and proves that two bits of global randomness are certified when performing measurements A_2 and B_7. □

5.1.4. Local randomness certification with POVMs

When considering POVMs instead of projective measurements, it is possible to extract up to 2 local random bits from a two-qubit state as shown in [APVW16], and theoretically, up to 4 global random bits, although no scheme has yet been provided achieving this value. This is twice as much as what can be obtained with projective measurements. These values are explained by the fact that a POVM acting on a space of dimension 2 can always be decomposed as a convex sum of POVMs of at most 4 outputs, which means at most 2 local bits, and 4 global bits if a POVM is used on each side. In [APVW16], the state considered for randomness extraction is maximally entangled. Here, we adapt their proof to our case and show that two bits of local randomness can be certified from any partially entangled state $|\psi_\theta\rangle$ with $\theta\in]0,\pi/2]$.

Bob's extra measurement

Let us suppose that Alice and Bob perform a Bell experiment just like the scenario above, with measurements A_1, A_2, A_3 and $B_1,\ldots,B_6$ obeying relations (5.3)–(5.5), which allow them to make statements as derived above. In the present scenario, we wish to change Bob's ideal operator B_7 so that it is a POVM – thus, the condition (5.6) involving the extra operator B_7 has to be modified.

More precisely, the ideal measurement B_7 will be replaced by a four-outcome POVM and used to generate the randomness. If Alice and Bob share the partially entangled state $|\psi_\theta\rangle$ then Bob has access to the marginal state

$$\psi_\theta^{\mathrm{B}} = \tfrac{1}{2}\big(\mathbb{I} + \cos(\theta)Z\big)\,. \tag{5.54}$$

In order to certify two random bits by making measurements on this state, Bob's POVM will have to be extremal in the set of qubit measurements, i.e. it must not be possible to express it as a convex sum of POVMs other than itself. Fortunately it is relatively easy to derive POVMs satisfying these requirements. Any rank-one POVM $R^{\mathrm{id}} = \{R_b^{\mathrm{id}}\}$ with elements of the form

$$R_b^{\mathrm{id}} = \alpha_b \phi_b, \tag{5.55}$$

with $\alpha_b > 0$ is extremal provided that the pure states ϕ_b are linearly independent. An example of such a POVM is given by

$$R_1^{\mathrm{id}} = \frac{1}{4 + 4\cos(\theta)}\Big(\mathbb{I} + Z\Big) \tag{5.56}$$

and, for $b \in \{2, 3, 4\}$,

$$R_b^{\mathrm{id}} = \frac{3 + 4\cos(\theta)}{12 + 12\cos(\theta)}\Big(\mathbb{I} + \cos(\lambda)Z + \sin(\lambda)(\cos(\mu_b)X + \sin(\mu_b)Y)\Big) \tag{5.57}$$

with $\cos(\lambda) = -1/(3 + 4\cos(\theta))$, and for angles $\mu_b = (0°, 120°, 240°)$.

The randomness certification we wish to show is based on the fact that we can reconstruct a POVM performed by Bob, such as $\{R_b^{\mathrm{id}}\}$, from its correlations with Pauli measurements on Alice's side on the state $|\psi_\theta\rangle$. Writing our ideal POVM $\{R_b^{\mathrm{id}}\}$ as

$$R_b^{\mathrm{id}} = r_b^{\mu}\sigma_\mu \tag{5.58}$$

in the identity and Pauli basis $\{\sigma_\mu\} = \{\mathbb{I}, X, Y, Z\}$, where we use implicit summation over the repeated index μ, we get

$$\langle \sigma_\mu \otimes R_b^{\mathrm{id}} \rangle_{\psi_\theta} = r_{b\mu} = \eta_{\mu\nu} r_b^{\nu} \tag{5.59}$$

where $\eta_{\mu\nu} = \langle \sigma_\mu \otimes \sigma_\nu \rangle_{\psi_\theta}$. For $\theta \neq 0$ one can verify that the $\eta_{\mu\nu}$s make up the components of an invertible matrix (e.g., its determinant is $-\sin(\theta)^4$). The conditions (5.59) thus uniquely identify the POVM elements R_b^{id}.

Let us go back to the device-independent setting where the actual measurement B_7, which we denote $B_7 = \{R_b\}$, is unknown. Condition (5.6) can be replaced by Alice and Bob checking that the local and two-body statistics are compatible with the ideal qubit POVM $\{R_b^{\mathrm{id}}\}$, i.e., compatible with (5.59):

$$\langle A_\mu \otimes R_b \rangle_\Psi = \langle \sigma_\mu \otimes R_b^{\mathrm{id}} \rangle_{\psi_\theta} = r_{b\mu} \tag{5.60}$$

where $A_\mu = (\mathbb{I} \otimes \mathbb{I}, X \otimes \mathbb{I}, Y \otimes A_Y, Z \otimes \mathbb{I})$ are the identity and Alice's measurements. In what follows, it will be useful to note that these can all be expressed together as

$$A_\mu = \sigma_\mu \otimes A_+ + \sigma_\mu^* \otimes A_- \tag{5.61}$$

where $A_\pm$ are the positive and negative parts of A_Y, such that $\mathbb{I}_{\mathrm{A'}} = A_+ + A_-$ and $A_Y = A_+ - A_-$, and σ_μ^* is the complex conjugate of σ_μ.

2 bits of local randomness

The condition (5.60) gives sufficient information about the measurement $\{R_b\}$ to show that it yields a uniformly random outcome. Let us model the problem explicitly in the adversarial picture and suppose that Alice and Bob share a purification $|\Psi\rangle = |\psi_\theta\rangle \otimes |\chi\rangle_{A'B'E}$ of the state identified by the Bell test with the eavesdropper Eve, who attempts to guess Bob's outcome. The associated guessing probability is:

$$P_{\text{guess}}(B_7|\mathrm{E}) = \sum_b \mathrm{Tr}\big[\Psi_{\mathrm{BB'E}}(R_b \otimes \Pi_{e=b})\big] \tag{5.62}$$

where $\{\Pi_e\}$ is a four-outcome POVM performed by Eve. Inserting $\mathbb{I}_{\mathrm{A'}} = A_+ + A_-$ we can rewrite the guessing probability as

$$\begin{aligned} P_{\text{guess}}(B_7|\mathrm{E}) &= \sum_{ab} \mathrm{Tr}\big[\Psi_{\mathrm{A'BB'E}}(A_a \otimes R_b \otimes \Pi_b)\big] \\ &= \sum_{ab} p_{ab}\, \mathrm{Tr}\big[\psi_\theta^{\mathrm{B}}\, R_{b|ab}\big] \,, \end{aligned} \tag{5.63}$$

$a \in \{\pm\}$, where in the second line we introduced probabilities p_{ae} and POVM elements $R_{b|ae}$ on the 'B' system defined by

$$p_{ae} = \mathrm{Tr}\big[(A_a \otimes \mathbb{I}_{\mathrm{BB'}} \otimes \Pi_e)(\mathbb{I}_{\mathrm{B}} \otimes \chi_{\mathrm{A'B'E}})\big] \,, \tag{5.64}$$

$$p_{ae} R_{b|ae} = \mathrm{Tr}_{\mathrm{A'B'E}}\big[(A_\pm \otimes R_b \otimes \Pi_e)(\mathbb{I}_{\mathrm{B}} \otimes \chi_{\mathrm{A'B'E}})\big] \,. \tag{5.65}$$

For $p_{ae} \neq 0$ we can see that the $R_{b|ae}$s defined this way form a POVM. Expanding R_b as

$$R_b = \sigma_\mu \otimes R_b^\mu \,, \tag{5.66}$$

we can identify the $R_{b|ae}$s by

$$p_{ae} R_{b|ae} = \sigma_\mu \langle A_a \otimes R_b^\mu \otimes \Pi_e \rangle_{\mathrm{A'B'E}} \,. \tag{5.67}$$

At this point we consider what we learn from the constraint $\langle A_\mu \otimes R_b \rangle = r_{b\mu}$. Multipying both sides by $\sigma^\mu = \eta^{\mu\nu}$ where $(\eta^{\mu\nu})$ is the matrix inverse of $(\eta_{\mu\nu})$ and then substituting in (5.66) we get

$$\begin{aligned} R_b^{\text{id}} &= \sigma^\mu \langle A_\mu \otimes R_b \rangle \\ &= \sigma^\mu \langle \sigma_\mu \otimes \sigma_\nu \rangle_{\psi_\theta} \langle A_+ \otimes R_b^\nu \rangle_{\text{A}'\text{B}'} + \sigma^\mu \langle \sigma_\mu^* \otimes \sigma_\nu \rangle_{\psi_\theta} \langle A_- \otimes R_b^\nu \rangle_{\text{A}'\text{B}'} \\ &= \sigma_\mu \langle A_+ \otimes R_b^\mu \rangle_{\text{A}'\text{B}'} + \sigma_\mu^* \langle A_- \otimes R_b^\mu \rangle_{\text{A}'\text{B}'} \\ &= \sum_e p_{+e} R_{b|+e} + \sum_e p_{-e} R_{b|-e}^* \,, \end{aligned} \tag{5.68}$$

where we used that $\sigma_\mu^* = \pm\sigma^\mu$ in the same way as σ_μ and, in the last line, $R_{b|-e}^*$ is the complex conjugate of $R_{b|-e}$. Comparing the first and last lines and using that $\{R_b^{\text{id}}\}$ is supposed to be extremal, we conclude

$$R_{b|+e} = R_b^{\text{id}} \qquad \text{and} \qquad R_{b|-e} = R_b^{\text{id}\,*} \tag{5.69}$$

(if $p_{ab} = 0$, we can set $R_{b|ae}$ to whatever we want). Using this in (5.63), we finally find

$$\begin{aligned} P_{\text{guess}}(B_7|\text{E}) &= \sum_b p_{+b} \operatorname{Tr}\bigl[\psi_\theta^{\text{B}} R_b^{\text{id}}\bigr] + \sum_b p_{-b} \operatorname{Tr}\bigl[\psi_\theta^{\text{B}} R_b^{\text{id}\,*}\bigr] \\ &= 1/4 \end{aligned} \tag{5.70}$$

for the local guessing probability, which means 2 random bits.

5.1.5. Discussion

To sum up, we found a scheme that certifies two bits of global randomness from any partially entangled state of two qubits, thus closing the open question of [AMP12]. We also showed how an adaptation of our scheme could certify two bits of local randomness by replacing the seventh measurement of Bob by an extremal four-outcome POVM. This scheme has the advantage of being valid for any angle θ describing $|\psi_\theta\rangle$. It may however not be optimal in terms of number of measurement choices. Finally, let us note that our result can also be seen as a self-test based on the combination of three Bell inequalities.

5.2. An approach based on the tilted Elegant inequality

In this section, we present a second approach to the question, in which we introduce a modified version of the so-called Elegant Bell inequality, which is valid for three measurement choices on Alice's side and four on Bob's side, with two outcomes per each measurement. We then find a tight quantum bound on those tilted Elegant inequalities valid when only qubit systems are considered. The corresponding qubit strategy is such that Alice makes measurements X, Y, and Z on the state $|\psi_\theta\rangle$, similarly to the optimal strategy of Section 5.1. When measurements are not limited to qubits, the quantum bound remains valid for a range of angles θ, which we show by providing an SOS decomposition to the shifted Bell operator. Using this SOS decomposition, we propose a self-testing procedure for Alice's measurements and the state. Outside of this range of θ, the situation remains unknown.

5.2.1. Elegant Bell inequality and its modification

In [Gis09], Gisin describes a Bell inequality with the interesting property that it is violated with qubit measurements using all three dimensions of the Bloch sphere. As argued in Section 5.1.1, this makes the Bell expression a good starting point for randomness certification from states $|\psi_\theta\rangle$. It is called the elegant Bell inequality:

$$\begin{aligned} S_{\text{el}} &= \langle A_1(B_1+B_2-B_3-B_4)\rangle + \langle A_2(B_1-B_2+B_3-B_4)\rangle \\ &\quad +\langle A_3(B_1-B_2-B_3+B_4)\rangle \\ &\leq 6. \end{aligned} \tag{5.71}$$

Its Tsirelson bound was shown to be $\beta_Q = 4\sqrt{3}$ in [APVW16]. It can be attained by performing the measurements $A_1 = X$, $A_2 = Y$, $A_3 = Z$, and

$$B_1 = \frac{1}{\sqrt{3}}(X - Y + Z)\,, \tag{5.72a}$$

$$B_2 = \frac{1}{\sqrt{3}}(X + Y - Z)\,, \tag{5.72b}$$

$$B_3 = \frac{1}{\sqrt{3}}(-X - Y - Z)\,, \tag{5.72c}$$

$$B_4 = \frac{1}{\sqrt{3}}(-X + Y + Z) \tag{5.72d}$$

on the maximally entangled state $|\phi_+\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$. We introduce a titled version of the Elegant Bell inequality, identified by the family of Bell expressions

$$\begin{aligned} S_{\alpha,\beta} &= \alpha\langle A_3\rangle + \langle A_1(B_1+B_2-B_3-B_4)\rangle + \langle A_2(B_1-B_2+B_3-B_4)\rangle \\ &\quad +\beta\langle A_3(B_1-B_2-B_3+B_4)\rangle. \end{aligned} \tag{5.73}$$

This depends on free parameters α and β. For $\alpha, \beta \geq 0$, we can see that $S_{\alpha,\beta}$ has the classical bound:

$$\beta_C^{\alpha,\beta} = \begin{cases} \alpha + 2\beta + 4 & \text{if } \beta \leq 2, \\ \alpha + 4\beta & \text{if } \beta \geq 2. \end{cases} \tag{5.74}$$

5.2.2. Limitation to qubits

Let us constrain the dimension of our problem and consider only two-qubit states. Measurements are then described in the basis $\{\mathbb{I}, X, Y, Z\}$. We first give a quantum strategy, and then show that it is the optimal one for qubits.

Qubit strategy

Recall the expression (5.2) for the density operator $\psi_\theta = |\psi_\theta\rangle\langle\psi_\theta|$:

$$\psi_\theta = \frac{1}{4}\Big[\mathbb{I}\otimes\mathbb{I} + \cos\theta\big(\mathbb{I}\otimes Z + Z\otimes\mathbb{I}\big) + \sin\theta\big(X\otimes X - Y\otimes Y\big) + Z\otimes Z\Big] \tag{5.75}$$

This expression is important to keep in mind, as it brings simplifications when computing the expectation value $\mathrm{Tr}[\mathcal{S}_{\alpha,\beta}\,\psi_\theta]$, where $\mathcal{S}_{\alpha,\beta}$ denotes the Bell operator corresponding to $S_{\alpha,\beta}$. We compute it for the choice of measurements: $A_1 = X$, $A_2 = Y$, $A_3 = Z$, and

$$B_1 = \frac{1}{\sqrt{2}}\sin(\mu)(X - Y) + \cos(\mu)Z\,, \tag{5.76}$$

$$B_2 = \frac{1}{\sqrt{2}}\sin(\mu)(X + Y) - \cos(\mu)Z\,, \tag{5.77}$$

$$B_3 = \frac{1}{\sqrt{2}}\sin(\mu)(-X - Y) - \cos(\mu)Z\,, \tag{5.78}$$

$$B_4 = \frac{1}{\sqrt{2}}\sin(\mu)(-X + Y) + \cos(\mu)Z. \tag{5.79}$$

Compared to the optimal measurements for the non-modified Elegant Bell inequality, a free parameter μ was introduced in Bob's measurement. The result, depending on θ and μ, is:

$$S_{\alpha,\beta} = \alpha\cos(\theta) + 4\sqrt{2}\sin(\mu)\sin(\theta) + 4\beta\cos(\mu)\,. \tag{5.80}$$

Note that if we choose $\cos(\theta) = 1$ (the special case of the separable state), then the maximal value of (5.80) is limited to $\alpha + 4\beta$. This coincides with the classical bound (5.74) only for $\beta \geq 2$, which tells us that we will need to use values approaching or exceeding $\beta = 2$ if we hope to cover states close to the separable state.

Maximising (5.80) over both θ and μ, we find

$$S_{\alpha,\beta} = \sqrt{\frac{1}{2}(2+\beta^2)(32+\alpha^2)}, \tag{5.81}$$

provided that the parameters satisfy $\alpha\beta \leq 8$. This optimum is obtained when

$$\cos(\mu) = \beta\sqrt{\frac{32+\alpha^2}{32(2+\beta^2)}}, \qquad \cos(\theta) = \alpha\sqrt{\frac{2+\beta^2}{2(32+\alpha^2)}}. \tag{5.82}$$

The constraint $\alpha\beta \leq 8$ comes from requiring $\cos(\mu) \leq 1, \cos(\theta) \leq 1$. The relations above invert to

$$\alpha = \sqrt{32}\,\frac{\sin(\mu)}{\tan(\theta)}, \qquad \beta = \sqrt{2}\,\frac{\sin(\theta)}{\tan(\mu)}. \tag{5.83}$$

Bound for qubit measurements

Let us set $\beta \geq 2$, and show that the quantum expectation value (5.81) is the maximum that can be attained using only qubit measurements.

Lemma 5.3. *When restricting the dimension of the state in the Bell test to* 2×2*, i.e. two-qubit states, the maximal quantum value of Bell expression* $S_{\alpha,\beta}$ *is*

$$\beta_Q^{(2\times 2)} = \sqrt{\frac{1}{2}(2+\beta^2)(32+\alpha^2)}, \tag{5.84}$$

with $\alpha\beta \leq 8$ *and* $\beta \geq 2$.

Proof. To answer this question, we relate $S_{\alpha,\beta}$ to the family of tilted CHSH expressions I_β^α from [AMP12] (note that $I_\beta^{\alpha=1} = I_\beta$ is the expression that was used in Section 5.1). The expression

$$I_\beta^\alpha = \alpha\langle A_1\rangle + \beta\big\langle A_1(B_1+B_2)\big\rangle + \big\langle A_2(B_1-B_2)\big\rangle \tag{5.85}$$

has the quantum upper bound

$$I_\beta^\alpha \leq \sqrt{(1+\beta^2)(4+\alpha^2)} \tag{5.86}$$

(at least) for $|\beta| \geq 1$ and $|\alpha\beta| \leq 2$. If we introduce a constant γ in front of the last term, i.e., we consider

$$I_{\beta,\gamma}^\alpha = \alpha\langle A_1\rangle + \beta\big\langle A_1(B_1+B_2)\big\rangle + \gamma\big\langle A_2(B_1-B_2)\big\rangle, \tag{5.87}$$

then the upper bound changes to

$$I^{\alpha}_{\beta,\gamma} \leq \sqrt{(\gamma^2+\beta^2)(4+\alpha^2/\gamma^2)} \tag{5.88}$$

for $|\beta| \geq |\gamma|$ and $|\alpha\beta| \leq 2\gamma^2$. The tilted elegant Bell expression $S_{\alpha,\beta}$ can be written in a way that looks like the sum of two I^{α}_{β} expressions:

$$\begin{aligned} S_{\alpha,\beta} = \alpha\langle A_3\rangle &+ \beta\big\langle A_3(B_1+B_4)\big\rangle + \big\langle(A_1+A_2)(B_1-B_4)\big\rangle \\ &- \beta\big\langle A_3(B_2+B_3)\big\rangle + \big\langle(A_1-A_2)(B_2-B_3)\big\rangle\,. \end{aligned} \tag{5.89}$$

Note that the terms A_1+A_2 and A_1-A_2 satisfy

$$(A_1+A_2)^2+(A_1-A_2)^2 = 4\mathbb{I}\,. \tag{5.90}$$

Given our hypothesis about the dimension of the problem, there are only two cases we need to consider: either one or both of A_1 and A_2 are the identity or both A_1 and A_2 are Pauli-type, i.e., $A_1 = \boldsymbol{a}_1\cdot\boldsymbol{\sigma}$ and $A_2 = \boldsymbol{a}_2\cdot\boldsymbol{\sigma}$ for vectors $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ of norm 1, and $\boldsymbol{\sigma} = (X,Y,Z)$.

Let us start with the first possibility. Without loss of generality, suppose $A_2 = \mathbb{I}$. The cases $A_2 = -\mathbb{I}$ and $A_1 = \pm\mathbb{I}$ are equivalent up to relabelling of inputs and outputs. $S_{\alpha,\beta}$ becomes

$$\begin{aligned} S_{\alpha,\beta} = \alpha\langle A_3\rangle &+ \beta\big\langle A_3(B_1+B_4)\big\rangle + \big\langle(A_1+\mathbb{I})(B_1-B_4)\big\rangle \\ &- \beta\big\langle A_3(B_2+B_3)\big\rangle + \big\langle(A_1-\mathbb{I})(B_2-B_3)\big\rangle\,. \end{aligned} \tag{5.91}$$

For any given state and measurement operators, we can view this as an average

$$S_{\alpha,\beta} = \frac{1}{2}S_1 + \frac{1}{2}S_2 \tag{5.92}$$

of two terms, with

$$\begin{aligned} S_1 = \alpha\langle A_3\rangle &+ \beta\big\langle A_3(B_1+B_4)\big\rangle + 2\big\langle A_1(B_1-B_4)\big\rangle \\ &- \beta\big\langle A_3(B_2+B_3)\big\rangle - 2\big\langle\mathbb{I}(B_2-B_3)\big\rangle \end{aligned} \tag{5.93}$$

and

$$\begin{aligned} S_2 = \alpha\langle A_3\rangle &+ \beta\big\langle A_3(B_1+B_4)\big\rangle + 2\big\langle\mathbb{I}(B_1-B_4)\big\rangle \\ &- \beta\big\langle A_3(B_2+B_3)\big\rangle + 2\big\langle A_1(B_2-B_3)\big\rangle\,. \end{aligned} \tag{5.94}$$

If we can find an upper bound for S_1 and S_2 then we will have an upper bound for $S_{\alpha,\beta}$. S_1 is just the sum of an $I^{\alpha}_{\beta,\gamma}$ expression with $\gamma = 2$ (on the first line) and remaining terms involving only B_2 and B_3 and only one nontrivial measurement on Alice's side (the second line). Using (5.88), S_1 is therefore bounded by

$$S_1 \leq \sqrt{4+\beta^2}\sqrt{4+\alpha^2/4}+2\beta\,. \tag{5.95}$$

The upper bound for S_2 is the same, so we arrive at the upper bound

$$S_{\alpha,\beta} \leq \sqrt{4+\beta^2}\sqrt{4+\alpha^2/4}+2\beta\,. \tag{5.96}$$

Applying the Cauchy-Schwarz inequality ($ax+yb \leq \sqrt{a^2+b^2}\sqrt{x^2+y^2}$) on the right-hand side finally gets us

$$\begin{aligned} S_{\alpha,\beta} &\leq \sqrt{4+\beta^2+\beta^2}\sqrt{4+\alpha^2/4+2^2} \\ &= \sqrt{\frac{1}{2}(2+\beta^2)(32+\alpha^2)}\,, \end{aligned} \tag{5.97}$$

which is the same as (5.84).

For the second possibility, i.e. for Pauli-type A_1 and A_2, we can define

$$A_1 + A_2 = 2\cos(\lambda)A_+\,, \qquad\qquad A_1 - A_2 = 2\sin(\lambda)A_- \tag{5.98}$$

for some angle λ and dichotomic and normalised $A_\pm$. Inserted in the expression for $S_{\alpha,\beta}$, this gives

$$\begin{aligned} S_{\alpha,\beta} = {}& \alpha\cos(\lambda)^2\langle A_3\rangle + \beta\big\langle A_3(B_1+B_4)\big\rangle + 2\cos(\lambda)\big\langle A_+(B_1-B_4)\big\rangle \\ &+ \alpha\sin(\lambda)^2\langle A_3\rangle - \beta\big\langle A_3(B_2+B_3)\big\rangle + 2\sin(\lambda)\big\langle A_-(B_2-B_3)\big\rangle\,, \end{aligned} \tag{5.99}$$

where we have split the first term $\alpha\langle A_3\rangle$ into $\alpha\cos(\lambda)^2\langle A_3\rangle + \alpha\sin(\lambda)^2\langle A_3\rangle$. Since we are interested in the range $\beta \geq 2$, the condition $|\beta| \geq |\gamma|$ associated with the rescaled expression $I^{\alpha}_{\beta,\gamma}$ above is satisfied for both $\gamma = 2\cos(\lambda)$ and $\gamma = 2\sin(\lambda)$. Likewise, the condition $|\alpha\beta| \leq 2\gamma^2$ reduces here to $|\alpha\beta| \leq 8$, which was exactly our constraint. Applying then the upper bound (5.88), we are able to recover (5.84):

$$\begin{aligned} S_{\alpha,\beta} &\leq \sqrt{4\cos(\lambda)^2+\beta^2}\sqrt{4+\alpha^2\cos(\lambda)^2/4} + \sqrt{4\sin(\lambda)^2+\beta^2}\sqrt{4+\alpha^2\sin(\lambda)^2/4} \\ &\leq \sqrt{4+2\beta^2}\sqrt{8+\alpha^2/4} \\ &= \sqrt{\frac{1}{2}(2+\beta^2)(32+\alpha^2)}\,. \end{aligned} \tag{5.100}$$

□

5.2.3. Sum-of-squares decomposition and Tsirelson bound for a range of partially entangled states

We ran numerical tests based on the NPA hierarchy (see Section 2.2.3) and found that while the quantum maximal violation of $S_{\alpha,\beta}$ corresponds to the qubit bound (5.84) for certain ranges of α and β, it is not the case for all values. Here, we show that the Tsirelson bound of $S_{\alpha,\beta}$ is indeed the qubit bound (5.84) for a certain range of parameters, by providing an SOS decomposition of the shifted Bell operator. Parameters α, β and μ, θ are related to each other by relations (5.82) and (5.83). In what follows, we mostly state our results in terms of μ and θ since they relate to the ideal state and measurements and thus have more physical meaning. Our result covers partially entangled states $|\psi_\theta\rangle$ with $\theta \gtrsim 1.23096$ radians (or about 70.52878 degrees).

Theorem 5.4. *The Tsirelson bound of Bell expression $S_{\alpha,\beta}$ is*

$$\beta_Q = \sqrt{\frac{1}{2}(2+\beta^2)(32+\alpha^2)}, \tag{5.101}$$

provided that

$$|\cos(\theta)| \leq 1/3, \tag{5.102}$$
$$\tan(\mu)^2 \leq \tfrac{1}{\sqrt{2}}\big(1+\cos(\theta)\big)\big(1-3\cos(\theta)\big)\big(\sqrt{2}\sin(\theta)-\cos(\theta)\big)\tfrac{1}{\sin(\theta)} \tag{5.103}$$

for $\alpha = \sqrt{32}\sin(\mu)/\tan(\theta)$ and $\beta = \sqrt{2}\sin(\theta)/\tan(\mu)$.

Proof. We give an SOS decomposition of the shifted Bell operator. Substituting α and β in terms of μ and θ, this means finding a decomposition for the operator:

$$\begin{aligned}\widetilde{\mathcal{S}_{\alpha,\beta}} = \beta_Q\mathbb{I} - \mathcal{S}_{\alpha,\beta} = {}& \sqrt{32}\big(1-\cos(\mu)^2\cos(\theta)^2\big)\mathbb{I} - \sqrt{32}\sin(\mu)^2\cos(\theta)A_3 \\ & - \sin(\mu)\sin(\theta)A_1(B_1+B_2-B_3-B_4) \\ & - \sin(\mu)\sin(\theta)A_2(B_1-B_2+B_3-B_4) \\ & - \sqrt{2}\cos(\mu)\sin(\theta)^2A_3(B_1-B_2-B_3+B_4)\,. \end{aligned}\tag{5.104}$$

Our decomposition is of the form:

$$\begin{aligned}\widetilde{\mathcal{S}_{\alpha,\beta}} = {}& \left|P_1^{++}\right|^2 + \left|P_2^{++}\right|^2 + \left|P_4^{++}\right|^2 + \left|P_1^{+-}\right|^2 + \left|P_2^{+-}\right|^2 + \left|P_3^{+-}\right|^2 \\ & + \left|P_1^{-+}\right|^2 + \left|P_2^{-+}\right|^2 + \left|P_3^{-+}\right|^2 + \left|P_1^{--}\right|^2 + \left|P_2^{--}\right|^2 + \left|P_3^{--}\right|^2 \end{aligned}\tag{5.105}$$

where we denote $|P|^2 = P^\dagger P$, and where the $P_k^{\pm\pm'}$s are twelve Hermitian operators of the form

$$\begin{aligned}
P_1^{++} &= \alpha_{11} R_1^{++}\,, && (5.106a)\\
P_2^{++} &= \alpha_{2*} R_1^{++} + \alpha_{2*} R_2^{++}\,, && (5.106b)\\
P_4^{++} &= \alpha_{41} R_1^{++} + \alpha_{42} R_2^{++} + \alpha_{44} R_4^{++}\,, && (5.106c)
\end{aligned}$$

$$\begin{aligned}
P_1^{+-} &= \beta_{11} R_1^{+-}\,, && (5.107a)\\
P_2^{+-} &= \beta_{2*} R_1^{+-} + \beta_{2*} R_2^{+-}\,, && (5.107b)\\
P_3^{+-} &= \beta_{32} R_2^{+-} + \beta_{33} R_3^{+-}\,, && (5.107c)
\end{aligned}$$

$$\begin{aligned}
P_1^{-+} &= \beta_{11} R_1^{-+}\,, && (5.108a)\\
P_2^{-+} &= \beta_{2*} R_1^{-+} + \beta_{2*} R_2^{-+}\,, && (5.108b)\\
P_3^{-+} &= \beta_{32} R_2^{-+} + \beta_{33} R_3^{-+}\,, && (5.108c)
\end{aligned}$$

$$\begin{aligned}
P_1^{--} &= \gamma_{11} R_1^{--}\,, && (5.109a)\\
P_2^{--} &= \gamma_{21} R_1^{--} + \gamma_{22} R_2^{--}\,, && (5.109b)\\
P_3^{--} &= \gamma_{32} R_2^{--} + \gamma_{33} R_3^{--}\,. && (5.109c)
\end{aligned}$$

The operators $R_k^{\pm\pm'}$ appearing in (5.106), (5.107), (5.108), and (5.109) are given by

$$\begin{aligned}
R_1^{++} &= 4\cos(\mu)\mathbb{I} - A_3(B_1 - B_2 - B_3 + B_4)\,, && (5.110a)\\
R_2^{++} &= 4\cos(\mu)A_3 - (B_1 - B_2 - B_3 + B_4)\,, && (5.110b)\\
R_3^{++} &= A_1(B_1 + B_2 - B_3 - B_4) - A_2(B_1 - B_2 + B_3 - B_4)\,, && (5.110c)\\
R_4^{++} &= 4\sqrt{2}\sin(\mu)\mathbb{I} - 4\sqrt{2}\sin(\mu)\cos(\theta)A_3\\
&\quad - \sin(\theta)A_1(B_1 + B_2 - B_3 - B_4)\\
&\quad - \sin(\theta)A_2(B_1 - B_2 + B_3 - B_4)\,, && (5.110d)
\end{aligned}$$

$$\begin{aligned}
R_1^{+-} &= 4\sqrt{2}\cos(\mu)\sin(\mu)A_2\\
&\quad - 2\cos(\mu)\sin(\theta)(B_1 - B_2 + B_3 - B_4)\\
&\quad - \sqrt{2}\sin(\mu)\cos(\theta)A_2(B_1 - B_2 - B_3 + B_4)\,, && (5.111a)\\
R_2^{+-} &= \sqrt{2}\cos(\mu)\cos(\theta)(B_1 - B_2 + B_3 - B_4)\\
&\quad - \sin(\mu)\sin(\theta)A_2(B_1 - B_2 - B_3 + B_4)\\
&\quad - \sqrt{2}\cos(\mu)A_3(B_1 - B_2 + B_3 - B_4)\,, && (5.111b)
\end{aligned}$$

$$R_3^{+-} = A_1(B_1 + B_2 + B_3 + B_4)\,, \tag{5.111c}$$

$$\begin{aligned} R_1^{-+} &= 4\sqrt{2}\cos(\mu)\sin(\mu)A_1 \\ &\quad - 2\cos(\mu)\sin(\theta)(B_1 + B_2 - B_3 - B_4) \\ &\quad - \sqrt{2}\sin(\mu)\cos(\theta)A_1(B_1 - B_2 - B_3 + B_4)\,, && (5.112a) \\ R_2^{-+} &= \sqrt{2}\cos(\mu)\cos(\theta)(B_1 + B_2 - B_3 - B_4) \\ &\quad - \sin(\mu)\sin(\theta)A_1(B_1 - B_2 - B_3 + B_4) \\ &\quad - \sqrt{2}\cos(\mu)A_3(B_1 + B_2 - B_3 - B_4)\,, && (5.112b) \\ R_3^{-+} &= A_2(B_1 + B_2 + B_3 + B_4)\,, && (5.112c) \end{aligned}$$

$$\begin{aligned} R_1^{--} &= B_1 + B_2 + B_3 + B_4\,, && (5.113a) \\ R_2^{--} &= A_1(B_1 - B_2 + B_3 - B_4) + A_2(B_1 + B_2 - B_3 - B_4)\,, && (5.113b) \\ R_3^{--} &= A_3(B_1 + B_2 + B_3 + B_4)\,. && (5.113c) \end{aligned}$$

They are all linearly independent and have the property that $R_k^{\pm\pm'}|\psi\rangle = 0$ when $|\psi\rangle = \cos(\theta/2)|00\rangle + \sin(\theta/2)|11\rangle$ and when the ideal measurements are used ($A_1 = X$, $A_2 = Y$, $A_3 = Z$, and B_y as given in (5.76) - (5.79)). Note that one of them, R_3^{++}, is unused in the SOS. The $R_k^{\pm\pm'}$ are grouped above according to whether or not they change sign under the transformations

$$T_1 : \begin{cases} A_1 \mapsto -A_1 \\ B_1 \mapsto -B_2 \\ B_2 \mapsto -B_1 \\ B_3 \mapsto -B_4 \\ B_4 \mapsto -B_3 \end{cases}, \qquad T_2 : \begin{cases} A_2 \mapsto -A_2 \\ B_1 \mapsto -B_3 \\ B_2 \mapsto -B_4 \\ B_3 \mapsto -B_1 \\ B_4 \mapsto -B_2 \end{cases}. \tag{5.114}$$

Specifically, the R_k^{++}s are unchanged by both transformations, the R_k^{-+}s change sign under T_1 only, the R_k^{+-}s change sign under T_2 only, and the R_k^{--}s change sign under both transformations.

The coefficients appearing in the expressions (5.106), (5.107), (5.108), and (5.109) for the SOS operators $P_k^{\pm\pm'}$ are

$$\alpha_{11} = \frac{2^{1/4}}{4}\,\frac{1}{\cos(\mu)}\sqrt{2\cos(\mu)^2\sin(\theta)^2 - \cos(2\mu)\big(\cos(\theta)^2 + 2\cos(\theta)\big) - 1}\,, \tag{5.115}$$

$$\alpha_{2*} = \frac{2^{1/4}}{4}\sqrt{\big(1 - \tan(\mu)^2\big)\cos(\theta)}\,, \tag{5.116}$$

$$\alpha_{41} = \frac{2^{1/4}}{4}\,, \tag{5.117}$$

$$\alpha_{42} = -\frac{2^{1/4}}{4}\big(1 - \tan(\mu)^2\big)\cos(\theta)\,, \tag{5.118}$$

$$\alpha_{44} = \frac{1}{4\;2^{1/4}}\tan(\mu)\,, \tag{5.119}$$

$$\beta_{11} = \frac{1}{4\;2^{3/4}}\frac{1}{\cos(\mu)}\sqrt{1 - \tan(\mu)^2 - \cos(\theta)\big(\sqrt{2}\sin(\theta) - \cos(\theta)\big)}\,, \tag{5.120}$$

$$\beta_{2*} = \frac{1}{4\sqrt{2}}\frac{1}{\cos(\mu)}\sqrt{\sin(\theta)\cos(\theta)}\,, \tag{5.121}$$

$$\beta_{32} = \frac{1}{4\sqrt{2}}\frac{1}{\cos(\mu)}\sqrt{\sin(\theta)\big(\sqrt{2}\sin(\theta) - \cos(\theta)\big)}\,, \tag{5.122}$$

$$\beta_{33} = -\frac{1}{4}\tan(\mu)\frac{\sin(\theta)}{\sqrt{\sin(\theta)\big(\sqrt{2}\sin(\theta) - \cos(\theta)\big)}}\,, \tag{5.123}$$

$$\gamma_{11} = \frac{2^{1/4}}{4}\sqrt{\big(1 + \cos(\theta)\big)\big(1 - 3\cos(\theta)\big) - \sqrt{2}\frac{\tan(\mu)^2\sin(\theta)}{\sqrt{2}\sin(\theta) - \cos(\theta)}}\,, \tag{5.124}$$

$$\gamma_{21} = \frac{2^{1/4}}{4}\sqrt{\cos(\theta)\big(1 + \cos(\theta)\big)}\,, \tag{5.125}$$

$$\gamma_{22} = \frac{1}{4\;2^{1/4}}\tan(\mu)\sin(\theta)\sqrt{\frac{\cos(\theta)}{1 + \cos(\theta)}}\,, \tag{5.126}$$

$$\gamma_{32} = \frac{1}{4\;2^{1/4}}\tan(\mu)\frac{\sin(\theta)}{\sqrt{1 + \cos(\theta)}}\,, \tag{5.127}$$

$$\gamma_{33} = \frac{2^{1/4}}{4}\sqrt{1 + \cos(\theta)}\,. \tag{5.128}$$

With these coefficients, the SOS decomposition (5.105) expands to the shifted Bell operator (5.104) as long as the coefficients above are real, i.e., when the expressions appearing under the various square roots are nonnegative. This condition is the one that restricts our range of angles θ, μ. A first restriction is that $\sin(\theta)$ and $\cos(\theta)$ are nonnegative. This is not a problem since it corresponds to the convention of taking θ in the range $[0, \pi/2]$, which we already did. Expression (5.122) for β_{32} means that $\sqrt{2}\sin(\theta) - \cos(\theta)$ should be nonnegative; together with the expression (5.124) for γ_{11} this implies that we are limited to values of μ satisfying

$$\tan(\mu)^2 \leq \frac{1}{\sqrt{2}}\big(1 + \cos(\theta)\big)\big(1 - 3\cos(\theta)\big)\big(\sqrt{2}\sin(\theta) - \cos(\theta)\big)\frac{1}{\sin(\theta)}\,. \tag{5.129}$$

Finally, the right-hand side of (5.129) must be nonnegative in order for (5.129) to be feasible, which requires that $1 - 3\cos(\theta) \geq 0 \Rightarrow \cos(\theta) \leq 1/3$. We have thus recovered conditions (5.102) and (5.103) of the statement of the theorem. Note that other expressions also imply constraints on μ (for example, expression (5.116) for α_{2*} requires $|\tan(\mu)| \leq 1$), but these are less restrictive than (5.129).

To conclude the proof, let us notice that the bound β_Q is tight, as it is attained by the qubit strategy presented in Section 5.2.2. □

5.2.4. Self-testing in the ideal case

Armed with the SOS decomposition just derived, we show that the maximal violation of the elegant Bell inequality $\mathcal{S}_{\alpha,\beta}$, provided an assumption on the regularisation of the observables, self-tests the partially entangled state $|\psi_\theta\rangle = \cos(\theta/2)|00\rangle + \sin(\theta/2)|11\rangle$ and the measurements X, Y, Z on Alice's side (as we saw, the three directions of the Bloch sphere are needed here for randomness certification). We present the self-test in the ideal case only. Note that it is valid only for the range (5.102) of angles θ. In this section, we adopt the self-testing notation introduced previously where A'_i, B'_i denote the physical measurements, while A_i, B_i denote the reference measurements.

Isometry and SOS relations

There is a subtlety in this self-test which has not appeared in the other self-tests in this thesis. Indeed, self-testing the observable $A_2 = Y$ up to local isometries only is not possible, and one has to add complex conjugation to the notion of equivalence between the physical and reference measurements. This is because quantum behaviours $\vec{p}$ are invariant under complex conjugation of the state and measurements. Hence, only a mixture of $A_2 = Y$ and $A_2 = Y^*$ can be self-tested. This question was studied for instance in [MM11], [ABB+17] and [BŠCA18b]. We proceed as in [BŠCA18b] and adapt their isometry to our case in Figure 5.1.

We choose for the gates of the circuit to be $X'_A = A'_1$, $Y'_A = A'_2$, and $Z'_A = A'_3$. On Bob's side the expressions are more complex:

$$X'_B = \frac{B'_1 + B'_2 - B'_3 - B'_4}{2\sqrt{2}\sin\mu}, \tag{5.130}$$

$$Y'_B = \frac{-B'_1 + B'_2 - B'_3 + B'_4}{2\sqrt{2}\sin\mu}, \tag{5.131}$$

$$Z'_B = \frac{B'_1 - B'_2 - B'_3 + B'_4}{4\cos\mu}. \tag{5.132}$$

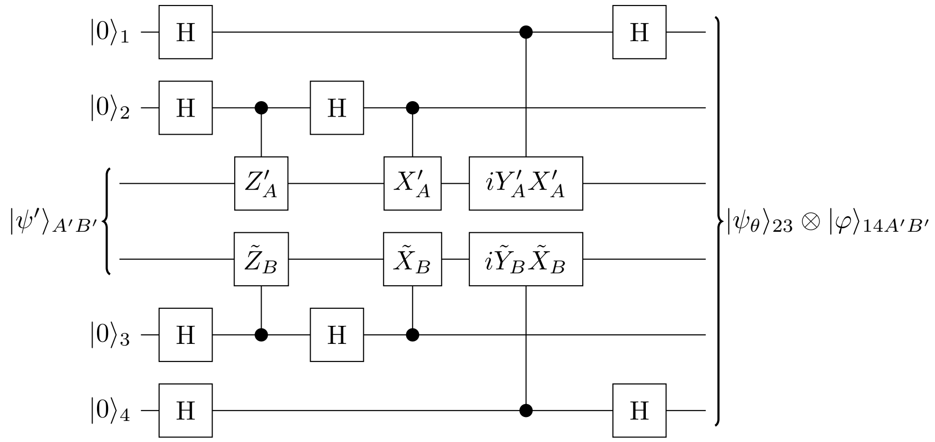

Figure 5.1.: Isometry Φ for our self-test, adapted from the initial swap gate in order to self-test observable Y. Two auxiliary systems are now used on each side. The new systems act as control spaces for possible complex conjugation or transposition. The gates of the circuit are functions of Alice and Bob's physical operators A'_x, B'_y. At the end of the circuit, we find the junk state $|\varphi\rangle$ in tensor product with the reference state $|\psi_\theta\rangle$.

One can verify that in the ideal case, those operators are indeed Pauli matrices X, Y, Z. On Alice's side, the operations are unitary, but on Bob's side they need to be regularised: we denote the regularised observables $\tilde{X}_B, \tilde{Y}_B$ and $\tilde{Z}_B$ (see Section 3.3.2). We assume that they act on the physical state like the non-regularised observables, i.e. $\tilde{X}_B|\psi'\rangle = X'_B|\psi'\rangle$, and the same for $\tilde{Y}_B$ and $\tilde{Z}_B$, and we leave the proof of this assumption as an open question. For clarity, since there is an exact correspondence between Alice's measurements and the gates, we will use the operators A'_i directly.

From SOS decomposition (5.105), when the maximal violation of $S_{\alpha,\beta}$ is observed, several relations can be derived. The following holds:

$$R_1^{++}|\psi'\rangle = 0 \Leftrightarrow (\mathbb{I} - A'_3\tilde{Z}_B)|\psi'\rangle = 0, \tag{5.133}$$

$$R_4^{++}|\psi'\rangle = 0 \Leftrightarrow \big(2\mathbb{I} - 2\cos(\theta)A'_3 - \sin(\theta)A'_1\tilde{X}_B + \sin(\theta)A'_2\tilde{Y}_B\big)|\psi'\rangle = 0, \tag{5.134}$$

$$R_1^{+-}|\psi'\rangle = 0 \Leftrightarrow (A'_2 + \sin(\theta)\tilde{Y}_B - \cos(\theta)A'_2\tilde{Z}_B)|\psi'\rangle = 0, \tag{5.135}$$

$$R_2^{+-}|\psi'\rangle = 0 \Leftrightarrow \big(-\cos(\theta)\tilde{Y}_B - \sin(\theta)A'_2\tilde{Z}_B + A'_3\tilde{Y}_B\big)|\psi'\rangle = 0, \tag{5.136}$$

$$R_1^{-+}|\psi'\rangle = 0 \Leftrightarrow (A'_1 - \sin(\theta)\tilde{X}_B - \cos(\theta)A'_1\tilde{Z}_B)|\psi'\rangle = 0, \tag{5.137}$$

$$R_2^{-+}|\psi'\rangle = 0 \Leftrightarrow \big(\cos(\theta)\tilde{X}_B - \sin(\theta)A'_1\tilde{Z}_B - A'_3\tilde{X}_B\big)|\psi'\rangle = 0, \tag{5.138}$$

$$R_2^{--}|\psi'\rangle = 0 \Leftrightarrow \big(-A'_1\tilde{Y}_B + A'_2\tilde{X}_B\big)|\psi'\rangle = 0. \tag{5.139}$$

Moreover, note that we will be using the fact that $M^2 = \mathbb{I}$ for M unitary and hermitian, which is the case for A'_1, A'_2, A'_3, and the regularised $\tilde{X}_B, \tilde{Y}_B$ and $\tilde{Z}_B$. It implies in particular $(\mathbb{I}+M)(\mathbb{I}+M) = 2(\mathbb{I}+M)$ and $(\mathbb{I}+M)(\mathbb{I}-M) = 0$. We also remind that operators on Alice's side commute with operators on Bob's side. Writing $c = \cos(\theta/2)$ and $s = \sin(\theta/2)$, these relations imply:

$$(5.133) \Rightarrow A'_3|\psi'\rangle = \tilde{Z}_B|\psi'\rangle, \tag{5.140}$$

$$s \times (5.135) - c \times (5.136) \Rightarrow sA'_2(\mathbb{I} + A'_3)|\psi'\rangle = -c\tilde{Y}_B(\mathbb{I} - A'_3)|\psi'\rangle, \tag{5.141}$$

$$s \times (5.137) - c \times (5.138) \Rightarrow sA'_1(\mathbb{I} + A'_3)|\psi'\rangle = c\tilde{X}_B(\mathbb{I} - A'_3)|\psi'\rangle, \tag{5.142}$$

$$(5.139) \Rightarrow A'_2A'_1|\psi'\rangle = \tilde{Y}_B\tilde{X}_B|\psi'\rangle, \tag{5.143}$$

$$\tilde{Y}_B \times (5.134) - 2\sin(\theta) \times (5.135) + 2\cos(\theta) \times (5.136) \Rightarrow A'_2A'_1|\psi'\rangle = -A'_1A'_2|\psi'\rangle, \tag{5.144}$$

$$\tilde{Y}_B \times (5.134) - 2\sin(\theta) \times (5.137) + 2\cos(\theta) \times (5.138) \Rightarrow \tilde{Y}_B\tilde{X}_B|\psi'\rangle = -\tilde{X}_B\tilde{Y}_B|\psi'\rangle. \tag{5.145}$$

As we will only show self-testing of the measurements of Alice, what we need to prove is the following:

$$\Phi\big((A'_i \otimes \mathbb{I})|\psi'\rangle_{A'B'}|0000\rangle_{1234}\big) = (A_i \otimes \mathbb{I})|\psi_\theta\rangle_{23} \otimes |\varphi\rangle_{14A'B'}, \tag{5.146}$$

with $i = 1, 2, 3$ and $|\varphi\rangle$ the junk state. To do so, let us expand the action of the isometry from Figure 5.1 on the physical state:

$$
\begin{aligned}
&\Phi\big((A'_i \otimes \mathbb{I})|\psi'\rangle_{A'B'}|0000\rangle_{1234}\big) = \\
&\frac{1}{16}\Big[\Big(\underbrace{|00\rangle_{14}(\mathbb{I} + i\tilde{Y}_B\tilde{X}_B)(\mathbb{I} + iA'_2A'_1)}_{T_1} + \underbrace{|01\rangle_{14}(\mathbb{I} - i\tilde{Y}_B\tilde{X}_B)(\mathbb{I} + iA'_2A'_1)}_{T_2} \\
&+ \underbrace{|10\rangle_{14}(\mathbb{I} + i\tilde{Y}_B\tilde{X}_B)(\mathbb{I} - iA'_2A'_1)}_{T_3} + \underbrace{|11\rangle_{14}(\mathbb{I} - i\tilde{Y}_B\tilde{X}_B)(\mathbb{I} - iA'_2A'_1)}_{T_4}\Big) \\
&\otimes \Big(\underbrace{(\mathbb{I} + A'_3)(\mathbb{I} + \tilde{Z}_B)A'_i|\psi'\rangle_{A'B'}|00\rangle_{23}}_{V_1} + \underbrace{\tilde{X}_B(\mathbb{I} + A'_3)(\mathbb{I} - \tilde{Z}_B)A'_i|\psi'\rangle_{A'B'}|01\rangle_{23}}_{V_2} \\
&+ \underbrace{A'_1(\mathbb{I} - A'_3)(\mathbb{I} + \tilde{Z}_B)A'_i|\psi'\rangle_{A'B'}|10\rangle_{23}}_{V_3} + \underbrace{A'_1\tilde{X}_B(\mathbb{I} - A'_3)(\mathbb{I} - \tilde{Z}_B)A'_i|\psi'\rangle_{A'B'}|11\rangle_{23}}_{V_4}\Big)\Big].
\end{aligned}
\tag{5.147}
$$

Self-testing of the state $|\psi_\theta\rangle$

For state self-testing, we need to prove (5.146) with $A'_i = A_i = \mathbb{I}$. Equation (5.140) implies that the terms V_2 and V_3 are zero. Using equation (5.142), we get:

$$
V_1 + V_4 = 2(\mathbb{I} + A'_3)|\psi'\rangle|00\rangle + 2\frac{s}{c}(\mathbb{I} + A'_3)|\psi'\rangle|11\rangle. \tag{5.148}
$$

Letting the junk state be $|\varphi\rangle = \frac{1}{8c}[T_1 + T_2 + T_3 + T_4](\mathbb{I} + A'_3)|\psi'\rangle$, this proves:

$$
\Phi\big(|\psi'\rangle|0000\rangle\big) = |\varphi\rangle \otimes |\psi_\theta\rangle. \tag{5.149}
$$

The expression for the junk state $|\varphi\rangle$ can be simplified. Indeed, using (5.141), (5.142) and (5.145) on $\tilde{X}_B\tilde{Y}_B(\mathbb{I} + A'_3)|\psi'\rangle$, we show that:

$$
\tilde{Y}_B\tilde{X}_B(\mathbb{I} + A'_3)|\psi'\rangle = A'_2A'_1(\mathbb{I} + A'_3)|\psi'\rangle, \tag{5.150}
$$

and, using (5.141) and (5.142) on $\tilde{X}_B\tilde{Y}_BA'_2A'_1(\mathbb{I} + A'_3)|\psi'\rangle$, that:

$$
\tilde{Y}_B\tilde{X}_BA'_2A'_1(\mathbb{I} + A'_3)|\psi'\rangle = -(\mathbb{I} + A'_3)|\psi'\rangle. \tag{5.151}
$$

Developing $[T_1 + T_2 + T_3 + T_4](\mathbb{I} + A'_3)|\psi'\rangle$, we thus obtain:

$$
|\varphi\rangle = \frac{1}{4c}\big(|00\rangle(\mathbb{I} + iA'_2A'_1) + |11\rangle(\mathbb{I} - iA'_2A'_1)\big)(\mathbb{I} + A'_3)|\psi'\rangle. \tag{5.152}
$$

Self-testing of X ($A_i = A_1$)

When $i = 1$ in (5.146), equations (5.140) and (5.142) imply that the terms V_1 and V_4 are zero. Using the same relations, we get:

$$V_2 + V_3 = 2\frac{s}{c}(\mathbb{I} + A_3')|\psi'\rangle|01\rangle + 2(\mathbb{I} + A_3')|\psi'\rangle|10\rangle \tag{5.153}$$

$$= \frac{2}{c}(s(\mathbb{I} + A_3')|\psi'\rangle|01\rangle + c(\mathbb{I} + A_3')|\psi'\rangle|10\rangle) \tag{5.154}$$

$$= \frac{2}{c}(\mathbb{I} + A_3')|\psi'\rangle(X \otimes \mathbb{I})|\psi_\theta\rangle. \tag{5.155}$$

This proves:

$$\Phi\big((A_1' \otimes \mathbb{I})|\psi'\rangle|0000\rangle\big) = |\varphi\rangle(X \otimes \mathbb{I})|\psi_\theta\rangle \tag{5.156}$$

and concludes the self-testing of X on Alice's side.

Self-testing of Z ($A_i = A_3$)

When $i = 3$ in (5.146), since $A_3'(\mathbb{I} - A_3') = A_3' - \mathbb{I}$, the terms V_2 and V_3 are zero. Equations (5.140) and (5.142) imply:

$$V_1 + V_4 = 2(\mathbb{I} + A_3')|\psi'\rangle|00\rangle - 2A_1'\tilde{X}_B(\mathbb{I} - A_3')|\psi'\rangle|11\rangle \tag{5.157}$$

$$= \frac{2}{c}(c(\mathbb{I} + A_3')|\psi'\rangle|00\rangle - s(\mathbb{I} + A_3')|\psi'\rangle|11\rangle) \tag{5.158}$$

$$= \frac{2}{c}(\mathbb{I} + A_3')|\psi'\rangle(Z \otimes \mathbb{I})|\psi_\theta\rangle. \tag{5.159}$$

This proves:

$$\Phi\big((A_3' \otimes \mathbb{I})|\psi'\rangle|0000\rangle\big) = |\varphi\rangle(Z \otimes \mathbb{I})|\psi_\theta\rangle \tag{5.160}$$

and concludes the self-testing of Z on Alice's side.

Self-testing of Y ($A_i = A_2$)

When $i = 2$ in (5.146), equations (5.140) and (5.141) imply that the terms V_1 and V_4 are zero. The rest needs to be developed. Using equations (5.140), (5.141), (5.142) and (5.145) we get:

$$V_2 + V_3 = -2\frac{s}{c}\tilde{X}_B\tilde{Y}_B(\mathbb{I} + A_3')|\psi'\rangle|01\rangle + 2\tilde{X}_B\tilde{Y}_B(\mathbb{I} + A_3')|\psi'\rangle|10\rangle \tag{5.161}$$

$$= \frac{2}{c}(c|10\rangle - s|01\rangle)\tilde{X}_B\tilde{Y}_B(\mathbb{I} + A_3')|\psi'\rangle. \tag{5.162}$$

Using equations (5.150) and (5.145), we prove that:

$$A_2'A_1'\tilde{X}_B\tilde{Y}_B(\mathbb{I} + A_3')|\psi'\rangle = (\mathbb{I} + A_3')|\psi'\rangle. \tag{5.163}$$

This implies:

$$\begin{aligned} T_2(V_2+V_3) &= |01\rangle\frac{2}{c}(c|10\rangle - s|01\rangle)(\tilde{X}_B\tilde{Y}_B + iA_2'A_1'\tilde{X}_B\tilde{Y}_B - i\mathbb{I} + A_2'A_1')(\mathbb{I}+A_3')|\psi'\rangle \\ &= 0. \end{aligned} \tag{5.164}$$

We get similarly:

$$T_3(V_2+V_3) = 0. \tag{5.165}$$

Finally,

$$\begin{aligned} T_1(V_2+V_3) &= |00\rangle\frac{2}{c}(c|10\rangle - s|01\rangle)(\tilde{X}_B\tilde{Y}_B + iA_2'A_1'\tilde{X}_B\tilde{Y}_B + i\mathbb{I} - A_2'A_1')(\mathbb{I}+A_3')|\psi'\rangle \\ &= |00\rangle\frac{2}{c}(c|10\rangle - s|01\rangle)(-2A_2'A_1' + 2i\mathbb{I})(\mathbb{I}+A_3')|\psi'\rangle \end{aligned} \tag{5.166}$$

and

$$\begin{aligned} T_4(V_2+V_3) &= |11\rangle\frac{2}{c}(c|10\rangle - s|01\rangle)(\tilde{X}_B\tilde{Y}_B - iA_2'A_1'\tilde{X}_B\tilde{Y}_B - i\mathbb{I} - A_2'A_1')(\mathbb{I}+A_3')|\psi'\rangle \\ &= |11\rangle\frac{2}{c}(c|10\rangle - s|01\rangle)(-2A_2'A_1' - 2i\mathbb{I})(\mathbb{I}+A_3')|\psi'\rangle \end{aligned} \tag{5.167}$$

which implies

$$\begin{aligned} \Phi\big((A_2'\otimes\mathbb{I})|\psi'\rangle|0000\rangle\big) &= \frac{2}{c}(c|10\rangle - s|01\rangle)\Big(|00\rangle(-2A_2'A_1' + 2i\mathbb{I}) \\ &\qquad + |11\rangle(-2A_2'A_1' - 2i\mathbb{I})\Big)(\mathbb{I}+A_3')|\psi'\rangle \\ &= Z^1|\varphi\rangle(Y\otimes\mathbb{I})|\psi_\theta\rangle \end{aligned} \tag{5.168}$$

where Z^1 is the Pauli-Z gate applied on Alice's first ancillary qubit (as numbered in Figure 5.1), and recalling expression (5.152) for the junk state $|\varphi\rangle$. This concludes the self-testing of Y on Alice's side: according to the outcome of the Z measurement on the junk state, either Y or Y^* is measured on the reference state. This is the best that can be done in terms of self-testing measurement Y [BŠCA18b].

5.2.5. Randomness and discussion

To sum up, we presented a modification of the Elegant Bell inequality and we could prove that it is maximally violated by the partiallly entangled states of two qubits $|\psi_\theta\rangle$, for a range of $\theta \gtrsim 1.23096$ radians. We did so by providing an explicit SOS decomposition, the level of which is $1 + AB$ (order 1 in operators of Alice and Bob, plus products of A and B). Note that our numerical tests indicate that this Tsirelson bound is valid for a larger range of θ than the one proven by the SOS decompositions. It may in principle be possible to find an SOS decomposition to cover a larger range of angles, however it would definitely not cover the whole range of θ, since we also found numerically that for some values of θ the maximal quantum violation is attained by systems of local dimension 4. Also, we believe that finding such an SOS decomposition would require a larger order, and obtaining level $1 + \mathrm{AB}$ was already a quite large problem. In fact, we used methods similar to [BP15] and [WBA18] for its derivation. In a few words, the idea is to write the general form of a candidate SOS decomposition in terms of unknown parameters with the help of the symmetries of the problem, assert that the decomposition should expand to the shifted Bell operator, and then look for parameters for which the assertion becomes true.

Then, we used our SOS decomposition to prove self-testing of state $|\psi_\theta\rangle$ and of measurements X, Y, Z on Alice's side, provided that the regularised observables act on the state as the non-regularised ones. Our result could in principle be used to perform randomness certification. We do not do it here, but the method would be similar to Section 5.1, adding an extra measurement B_5 on Bob's side aligned with $A_2 = Y$, which would then be used along Alice's measurement $A_1 = X$ to produce randomness.

5.3. Discussion

In this chapter, we were able to answer the open question of [AMP12] and certify two bits of global randomness from any partially entangled two-qubit state. We presented our scheme and a modification of it that certifies maximal local randomness using a POVM, as well as a second approach that we followed to answer the question which works for a range of partially entangled states.

These results complete our picture of the relations between nonlocality, entanglement and randomness, as pictured in Table 5.1. We proved that maximal randomness could be obtained from any level of two-qubit entanglement – in principle, all entangled two-qubit states could be seen as equally good resources for random number generation. However, this statement is slightly risky, as it is important to keep in mind that other factors may intervene. For instance, using the maximally entangled state requires less measurements choices from the users [DPA13]. Also, we expect that if we were to analyse the noise robustness of our scheme, it would decrease as the amount of entanglement decreases.

It could be interesting to study whether procedures with less measurements could be designed. In this sense, our second approach is interesting as it uses less

		$\|\phi^+\rangle$	$\|\psi_\theta\rangle$
Local	PROJ	1 bit [PAM+10]	1 bit [AMP12]
	POVM	2 bits [APVW16]	2 bits (our work)
Global	PROJ	2 bits [AMP12]	2 bits (our work)
	POVM	2.8997 bits [APVW16]	–

Table 5.1.: Summary of known results on randomness certified from two-qubit states. The best known lower bounds on the randomness are represented for the maximally entangled state and for partially entangled states (for the entire range of θ), as well as for both local and global randomness, considering projective measurements or POVMs. Our work solved the two cases that are highlighted in green. The bounds that are underlined correspond to the maximal possible amount of randomness – finding a scheme that certifies global randomness with POVMs is still an open question, both for $|\phi^+\rangle$ and $|\psi_\theta\rangle$.

measurements than the first one. A more general open question concerns global randomness certification with POVMs – can a scheme be found that guarantees 4 bits of local randomness from two-qubit states? As shown in Table 5.1, this has not been achieved so far with the maximally entangled state, which would be a good point to start from before considering partially entangled states.

6. Overview and outlook

This thesis is dedicated to device-independent protocols, and more specifically, to the Bell inequalities on which the success of these protocols rests. We have studied methods for constructing Bell expressions, analysed their properties and examined their applications to protocols such as quantum key distribution, self-testing, and randomness certification. We started with the chained Bell inequalities, then examined the CGLMP/BKP expressions and designed our own family of Bell inequalities, which we had the opportunity to see tested in an experiment. Later, we studied the tilted CHSH expressions, and found a modified version of the Elegant Bell inequality. We used a variety of techniques in this thesis, numerical as well as analytical, such as the SWAP method and sum-of-squares decompositions. Our results also highlight connexions between different device-independent protocols, for instance how some self-testing proofs can help certify randomness. In this chapter, we summarise our results and discuss open questions and directions for future research.

Chained Bell inequalities: self-testing and randomness certification

In Chapter 3, we designed robust self-testing protocols based on the chained Bell inequalities. The self-test of the measurements is particularly interesting, as the optimal measurements of the chained Bell inequalities span the whole X-Z plane of the Bloch sphere in the limit of a large number of inputs. Our proofs rely on SOS decompositions of first and second order. By proving that the chained Bell inequalities are useful for self-testing, we showed that their maximal violation is unique, up to the self-testing notion of equivalence. This result completed the proof of [DPA13] for certifying two global random bits from the singlet state. We also gave an alternative proof of the latter statement.

Our protocol could be improved by finding better robustness bounds, in particular by improving the scaling with the number of inputs. A potential approach could follow the work of [Kan16], whose recently introduced (or "revived") formalism has provided excellent robustness bounds. Also, it would be interesting to see if our protocols can be generalised to a scenario for many outputs. Candidate Bell inequalities would be the BKP inequalities [BKP06] and our family of Bell inequalities from Chapter 4, since they both reduce to the chained Bell inequalities when the number of outputs is set to two.

Bell inequalities tailored to maximally entangled states

In Chapter 4, we employed a method to derive adequate Bell inequalities based on the desired optimal quantum realisation (here, maximally entangled states). Our family of Bell inequalities is remarkable as it is valid for any number of inputs and outputs, and, moreover, its classical, quantum and no-signalling bounds can all be proven and obtained as analytical functions of the number of inputs and outputs. Our proof for the quantum bound rests on an SOS decomposition of order one. We argued how our Bell inequalities could be used for self-testing, randomness certification and quantum key distribution, giving examples for the case of three outcomes. In the case of self-testing, we used the numerical SWAP method from [YVB+14]. We then presented a generalisation of our family of Bell inequalities to many parties and studied their properties. We also considered the question of modifying our Bell inequality in the special case of two inputs and three outputs, in order to obtain a family of Bell inequalities suited to a class of partially entangled states of two qutrits. Finally, we presented the results of our experimental collaboration where violations of our inequalities were measured and self-testing and randomness certification were performed.

In the future, we are expecting to prolong this experimental collaboration in order to test the multipartite version of our Bell inequalities. We believe that one of the clearest open questions concerns self-testing: can analytical procedures be designed that would be valid for a general scenario? Such a self-testing result would imply randomness certification by proving that the maximal violation is unique – this is a necessary condition to apply the method of [DPA13] for which our Bell inequalities possess enough symmetries. We also briefly considered how our Bell expressions could be used for quantum key distribution, and we believe that a complete work on DIQKD from high dimensional states could be very interesting. Finally, we find particularly appealing the idea of having general Bell expressions tailored to classes of entangled states, so that, according to what state can be best generated in a given experimental setup, the optimal Bell expression could easily be selected. This idea would require expanding the preliminary work that we did for qutrit states.

Randomness from partially entangled states

In Chapter 5, we answered an open question from [AMP12] and showed that maximal randomness could be certified from any partially entangled state of two qubits: more specifically, two bits of global randomness with projective measurements and two bits of local randomness with POVMs. Our results complete the picture on the relation between randomness and entanglement for qubits. To that end, we used a CHSH inequality in combination with two tilted CHSH inequalities from which we could derive self-testing statements. We also presented a second approach to the question, which employs fewer measurements choices. We found a tilted version of the Elegant Bell inequality and showed that it is maximally violated by partially entangled states, for a certain range of those states. We did this by providing an SOS decomposition of the Bell operator of level $1 + AB$, and we used this decomposition to propose a self-testing procedure for the validity range of our results.

Although we showed that, if entanglement is seen as a resource to produce random numbers, any amount of qubit entanglement is equivalent, it is important to note that different resources are required to produce this randomness. For instance, more measurement choices are needed for partially entangled states than for the maximally entangled state. In future work, it would be interesting to find the minimal amount of measurement choices that are necessary, as well as to analyse the resistance to noise of our schemes. This may complete our view of the relation between entanglement and randomness, as states more weakly entangled may have lower resistance to noise, or may require more measurement choices than states containing more entanglement. In general, randomness in quantum information remains a perplexing subject that deserves being studied further in various scenarios (also in scenarios different from the standard Bell test). An interesting question concerns the certification of randomness using higher-dimensional states, as we commented in the results of Chapter 4. Also, we still lack a scheme to certify the maximal amount of global randomness from qubits using POVMs (four bits), which is a question worth investigating.

A. Tables

m d	2	3	4	5	6
2	1.414	1.299	1.232	1.189	1.159
3	1.291	1.214	1.167	1.137	1.116
4	1.252	1.186	1.146	1.120	1.102
5	1.233	1.173	1.136	1.112	1.095
6	1.222	1.165	1.130	1.107	1.091

Table A.1.: Numerical values of the ratio $\widetilde{\beta}_Q/\widetilde{\beta}_C$ between the quantum and classical bounds of $\widetilde{I}_{m,d}$ for low number of inputs m and outputs d. For $m = d = 2$, one recovers the well-known CHSH $\sqrt{2}$ ratio.

m d	2	3	4	5	6
2	1.414	1.155	1.082	1.051	1.035
3	1.366	1.137	1.073	1.046	1.031
4	1.342	1.128	1.069	1.043	1.029
5	1.328	1.123	1.066	1.041	1.028
6	1.319	1.120	1.064	1.040	1.027

Table A.2.: Numerical values of the ratio $\widetilde{\beta}_{NS}/\widetilde{\beta}_Q$ between the no-signalling and quantum bounds of $\widetilde{I}_{m,d}$ for low number of inputs m and outputs d. For $m = d = 2$, one recovers the well-known CHSH $\sqrt{2}$ ratio.

	$d=2$	$d=3$	$d=4$
$\beta_C^{3,3,d}$	$13/\sqrt{3}$	$\frac{1}{6\sqrt{3}}(13\cot(\frac{\pi}{18})$ $-17\tan(\frac{\pi}{9}) - 4\tan(\frac{2\pi}{9}))$	$\frac{-10+17\sqrt{2}+14\sqrt{6}}{4\sqrt{3}}$
$\beta_C^{4,2,d}$	$\frac{5}{2}(\cot(\frac{\pi}{8})$ $+\tan(\frac{\pi}{8}))$	$\frac{10}{\sqrt{3}} + \frac{5}{6}(-3+\sqrt{3})$	$\frac{1}{8}(10\cot(\frac{\pi}{16}) - 5\cot(\frac{3\pi}{16})$ $+16\tan(\frac{\pi}{16}) + \tan(\frac{3\pi}{16}))$
$\beta_C^{4,3,d}$	$35/\sqrt{3}$	$\frac{1}{6\sqrt{3}}(7(5\cot(\frac{\pi}{18})$ $-7\tan(\frac{\pi}{9}) - 2\tan(\frac{2\pi}{9})))$	/

Table A.3.: Analytical expression of the classical bound of $I_{N,m,d}$, for a few values of N, m, d. For $N=4$, $m=3$ and $d=4$, we did not obtain the value as the problem was computationally expensive.

	$d=2$	$d=3$	$d=4$
$\beta_C^{3,2,d}$	4.2426	3.0416	3.5953
$\beta_S^{3,2,d}$	4.2426	3.0416	3.5953
$\beta_C^{3,3,d}$	7.5056	6.1760	6.9765
$\beta_S^{3,3,d}$	8.6603	7.3132	8.1115
$\beta_C^{4,2,d}$	7.0711	4.7169	5.8301
$\beta_S^{4,2,d}$	8.4853	6.0829	7.1905
$\beta_C^{4,3,d}$	20.2073	16.2537	/
$\beta_S^{4,3,d}$	25.9808	21.9394	24.3345

Table A.4.: Numerical values of the Svetlichny and the classical bound of $I_{N,m,d}$, for a few values of N, m, d. When $N=3$, $m=2$, the two bounds are the same. For $N=4$, $m=3$ and $d=4$, we did not obtain the value as the problem was computationally expensive.

d	CGLMP	$\tilde{I}_d$
2	(2) 2.810±0.014 {2.828}	(1.414) 1.987±0.010 {2}
3	(2) 2.845±0.012 {2.873}	(3.098) 3.978±0.015 {4}
4	(2) 2.867±0.014 {2.896}	(4.793) 5.978±0.032 {6}
5	(2) 2.763±0.014 {2.910}	(6.489) 7.652±0.031 {8}
6	(2) 2.629±0.010 {2.920}	(8.187) 8.883±0.029 {10}
7	(2) 2.532±0.013 {2.927}	(9.884) 10.645±0.029 {12}
8	(2) 2.650±0.012 {2.932}	(11.581) 12.740±0.044 {14}

Table A.5.: Experimental values of CGLMP and $\widetilde{I}_d$ for $d = 2, \ldots 8$, given with experimental errors. Values in (*) refer to the classical bound; those in {*} refer to theoretical bounds for d-dimensional maximally entangled states (for $\widetilde{I}_d$, this means the Tsirelson bound). Errors are given by photon Poissonian noise.

$\gamma = 0.7923$		$\gamma = 0.9$		$\gamma = 1$	
$J_{2,2,3}(\xi)$	Min. fidelity	$J_{2,2,3}(\xi)$	Min. fidelity	$J_{2,2,3}(\xi)$	Min. fidelity
2.9149	1	3.0392	1	3.1547	1
2.9049	0.8193	3.0292	0.8189	3.1440	0.7992
2.8949	0.6638	3.0192	0.6615	3.1340	0.6372
2.8849	0.5319	3.0092	0.5273	3.1240	0.4993
2.8749	0.4207	2.9992	0.4138	3.1140	0.3823
2.8649	0.3276	2.9892	0.3187	3.1040	0.2871
2.8549	0.2500	2.9792	0.2398	3.0940	0.2082
2.8449	0.1858	2.9692	0.1748	3.0840	0.1446
2.8349	0.1334	2.9592	0.1223	3.0740	0.0945
2.8249	0.0914	2.9492	0.0807	3.0640	0.0564
2.8149	0.0585	2.9392	0.0488	3.0540	0.0289

Table A.6.: Minimum fidelity between the physical states in the black boxes and the states $|\psi_{0.7923}\rangle$, $|\psi_{0.9}\rangle$ and $|\psi_1\rangle$ respectively, versus the violation of the corresponding $J_{2,2,3}(\xi)$ with $\xi = 1$, $\xi = 0.6451$, and $\xi = \frac{\sqrt{3}-1}{2}$ respectively. At the maximal violation, the fidelity is equal to 1, meaning that the quantum state used in the Bell experiment must be equal to the reference state. For lower violations, the fidelity decreases. This data is used to plot the fidelity curves in Figure 4.9.

$\gamma = 0.7923$		$\gamma = 0.9$		$\gamma = 1$	
$J_{2,2,3}(\xi)$	Min. fidelity	$J_{2,2,3}(\xi)$	Min. fidelity	$J_{2,2,3}(\xi)$	Min. fidelity
2.904	0.8051	3.036	0.9394	3.1507	0.9212
2.896	0.6804	3.030	0.8323	3.1420	0.7992
2.888	0.5711	3.024	0.7339	3.1333	0.6372

Table A.7.: Minimum fidelity between the physical states in the black boxes and the states $|\psi_{0.7923}\rangle$, $|\psi_{0.9}\rangle$ and $|\psi_1\rangle$ respectively, for experimentally observed values of the violation of the corresponding $J_{2,2,3}(\xi)$ with $\xi = 1$, $\xi = 0.6451$, and $\xi = \frac{\sqrt{3}-1}{2}$ respectively. This data is used to plot the data points and error bars in Figure 4.9.

	Global randomness		
d	lower value	mean value	higher value
2	0.8903	0.9687	1.0992
3	1.3308	1.4412	1.6130
4	1.5922	1.8227	2.1400
5	0.9500	1.0036	1.0606
6	0.3085	0.3284	0.3490
7	0.2835	0.3001	0.3172
8	0.4417	0.4707	0.5008
$d = 3, \gamma = 0.9$	1.4566	1.5415	1.6693
$d = 3, \gamma = 0.7923$	1.3981	1.4708	1.5651

Table A.8.: Global randomness $H_{\min}^{x,y}$ certified per round, based on the observed violation of $\widetilde{I}_d$ for different values of d. The lower (higher) values correspond to -(+)1σ confidence interval for the Bell value, calculated using Poissonian photon statistics. This data is used to plot Figure 4.10. We also report the certified randomness based on the observed values of $J_{2,2,3}(\xi)$, obtained with partially entangled qutrit states $|\psi_\gamma\rangle$.

B. Self-test based on the tilted CHSH expression

In this Appendix, we prove in details Lemma 5.1. We proceed by proving progressively more general self-testing results, first restricting to projective measurements on a bipartite pure qubit state, then generalising to arbitrary dimension using the Jordan lemma, then explicitly allowing for an underlying mixed state and non-projective measurements. The proof is inspired from the results of [AMP12]. See also [BP15] for a self-test of I_β based on SOS decompositions.

Qubit systems

The most general two-qubit pure state $|\psi\rangle$ has the form

$$|\psi\rangle = \cos\!\left(\tfrac{\theta}{2}\right)|00\rangle + \sin\!\left(\tfrac{\theta}{2}\right)|11\rangle\,, \tag{B.1}$$

for $0 \leq \theta \leq \pi/2$, in its Schmidt decomposition, while the most general projective measurements worth considering are

$$A = \boldsymbol{a}\cdot\boldsymbol{\sigma}\,, \qquad B = \boldsymbol{b}\cdot\boldsymbol{\sigma}\,, \tag{B.2}$$

$$A' = \boldsymbol{a}'\cdot\boldsymbol{\sigma}\,, \qquad B' = \boldsymbol{b}'\cdot\boldsymbol{\sigma} \tag{B.3}$$

with $\boldsymbol{\sigma} = \{X, Y, Z\}$ and $\|\boldsymbol{a}\| = \|\boldsymbol{a}'\| = \|\boldsymbol{b}\| = \|\boldsymbol{b}'\| = 1$, since we can't exceed the classical bound if any of the measurements are $\pm\mathbb{I}$. Recall also how the density operator of state (B.1) can be written in terms of the Pauli operators X, Y, Z:

$$\psi = \frac{1}{4}\Big[\mathbb{I}\otimes\mathbb{I} + \cos(\theta)\big(\mathbb{I}\otimes Z + Z\otimes\mathbb{I}\big) + \sin(\theta)\big(X\otimes X - Y\otimes Y\big) + Z\otimes Z\Big] \tag{B.4}$$

Let us write the expectation value of I_β as

$$I_\beta = \beta\cos(\theta)a_z + I_{CHSH} \tag{B.5}$$

where

$$I_{CHSH} = \big\langle A(B+B') + A'(B-B')\big\rangle = \boldsymbol{a}\cdot\mathbf{T}(\boldsymbol{b}+\boldsymbol{b}') + \boldsymbol{a}'\cdot\mathbf{T}(\boldsymbol{b}-\boldsymbol{b}'), \tag{B.6}$$

and

$$\mathbf{T} = \begin{bmatrix} \sin(\theta) & 0 & 0 \\ 0 & -\sin(\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix} . \tag{B.7}$$

Substituting now

$$\boldsymbol{b} + \boldsymbol{b}' = 2\cos\left(\tfrac{\mu}{2}\right)\boldsymbol{b}_+ \,, \qquad \boldsymbol{b} - \boldsymbol{b}' = 2\sin\left(\tfrac{\mu}{2}\right)\boldsymbol{b}_- \,, \tag{B.8}$$

where $\boldsymbol{b}_\pm$ are normalised and orthogonal and we take $\cos\left(\frac{\mu}{2}\right), \sin\left(\frac{\mu}{2}\right) \geq 0$,

$$\begin{aligned} I_{CHSH} &= 2\cos\left(\tfrac{\mu}{2}\right)\boldsymbol{a}\cdot\mathbf{T}\boldsymbol{b}_+ + 2\sin\left(\tfrac{\mu}{2}\right)\boldsymbol{a}'\cdot\mathbf{T}\boldsymbol{b}_- \\ &\leq 2\cos\left(\tfrac{\mu}{2}\right)\|\mathbf{T}\boldsymbol{b}_+\| + 2\sin\left(\tfrac{\mu}{2}\right)\|\mathbf{T}\boldsymbol{b}_-\| \\ &\leq 2\sqrt{\|\mathbf{T}\boldsymbol{b}_+\|^2 + \|\mathbf{T}\boldsymbol{b}_-\|^2} \\ &= 2\sqrt{\mathrm{Tr}\left[\mathbf{T}^2\left(\boldsymbol{b}_+{\boldsymbol{b}_+}^T + \boldsymbol{b}_-{\boldsymbol{b}_-}^T\right)\right]} \\ &\leq 2\sqrt{1+\sin(\theta)^2} \,, \end{aligned} \tag{B.9}$$

where the last line follows from the Von Neumann trace inequality. This inequality says that for A and B Hermitian operators, the trace of their product respects

$$\mathrm{Tr}[AB] \leq \sum_k a_k b_k \tag{B.10}$$

where a_k and b_k are the eigenvalues of A and B ordered from largest to smallest. Equality is attained if and only if there is a basis in which A and B are both diagonal and the ordering of their eigenvalues by magnitude match. Using (B.9) in (B.5):

$$\begin{aligned} I_\beta &\leq \beta\cos(\theta)a_z + 2\sqrt{1+\sin(\theta)^2} \\ &\leq \beta\cos(\theta) + 2\sqrt{1+\sin(\theta)^2} \\ &\leq 2\sqrt{2}\sqrt{1+\beta^2/4} \,. \end{aligned} \tag{B.11}$$

In order to attain the quantum bound $I_\beta = 2\sqrt{2}\sqrt{1+\beta^2/4}$, all of the inequalities used to get from (B.5) to (B.11) must hold with equality. Working backwards, we extract that

$$
\begin{aligned}
2\cos(\theta) &= \beta\sqrt{1+\sin(\theta)^2}\,, && \text{(B.12)}\\
\boldsymbol{a} &= \mathbf{1}_{\mathrm{z}}\,, && \text{(B.13)}\\
\boldsymbol{b}_{+} &= \mathbf{1}_{\mathrm{z}}\,, && \text{(B.14)}\\
\boldsymbol{b}_{-} &= \cos(\varphi)\mathbf{1}_{\mathrm{x}} - \sin(\varphi)\mathbf{1}_{\mathrm{y}}\,, && \text{(B.15)}\\
\boldsymbol{a}' &= \cos(\varphi)\mathbf{1}_{\mathrm{x}} + \sin(\varphi)\mathbf{1}_{\mathrm{y}}\,, && \text{(B.16)}\\
\cos\left(\tfrac{\mu}{2}\right)\sin(\theta) &= \sin\left(\tfrac{\mu}{2}\right). && \text{(B.17)}
\end{aligned}
$$

Under the conventions $\beta > 0$ and $0 \leq \theta_\beta, \frac{\mu_\beta}{2} \leq \frac{\pi}{2}$ that we are working with, these imply the relations (5.17) and (5.18) for θ_β and μ_β given in the main text. The remaining undetermined parameter φ can be set to 0 e.g. with the phase changes $|1\rangle_{\mathrm{A}} \mapsto e^{i\varphi}|1\rangle_{\mathrm{A}}$ and $|1\rangle_{\mathrm{B}} \mapsto e^{-i\varphi}|1\rangle_{\mathrm{B}}$, under which the Schmidt decomposition is invariant.

In the derivation above we started by expressing a general two-qubit state $|\psi\rangle$ in its Schmidt decomposition and have shown that, if the quantum bound is attained, the measurements must satisfy

$$
\begin{aligned}
A_1 &= Z\,, && \text{(B.18)}\\
A_2 &= \cos(\varphi)X + \sin(\varphi)Y\,, && \text{(B.19)}\\
B_1 + B_2 &\propto Z\,, && \text{(B.20)}\\
B_1 - B_2 &\propto \cos(\varphi)X - \sin(\varphi)Y && \text{(B.21)}
\end{aligned}
$$

with respect to the Schmidt basis. It is important to note that the converse also holds: if the quantum bound is attained with measurements satisfying these conditions then the state must be exactly $|\psi_\beta\rangle = \cos\left(\frac{\theta_\beta}{2}\right)|00\rangle + \sin\left(\frac{\theta_\beta}{2}\right)|11\rangle$. So the reasoning can be done this way: if the quantum bound is attained with qubits then there is a choice of bases in which $A_1 = Z$, $A_2 = X$, $B_1 + B_2 \propto Z$, and $B_1 - B_2 \propto X$, and this then determines that the state is $|\psi_\beta\rangle$ with respect to that choice of the bases.

Arbitrary dimension

According to the Jordan lemma the measurement operators A, A' and B, B' can be block diagonalised in their respective Hilbert spaces into blocks no larger than 2×2. We express the block diagonalisation as

$$
A = \sum_j A_j \otimes |j\rangle\langle j| \,\oplus\, A_\perp\,, \qquad \text{(B.22)}
$$

$$A' = \sum_j A'_j \otimes |j\rangle\langle j| \,\oplus\, A'_\perp \,, \tag{B.23}$$

$$B = \sum_k B_k \otimes |k\rangle\langle k| \,\oplus\, B_\perp \,, \tag{B.24}$$

$$B' = \sum_k B'_k \otimes |k\rangle\langle k| \,\oplus\, B'_\perp \,, \tag{B.25}$$

where A_j, A'_j, B_k, and B'_k are 2×2 operators and the operators with the '$\perp$' subscript collectively denote any 1×1 blocks. Note that this implies $[A_\perp, A'_\perp] = 0$ and $[B_\perp, B'_\perp] = 0$. With respect to this splitting of the Hilbert space we can express an arbitrary pure state as

$$|\Psi\rangle = \bigoplus_{mn} \sqrt{p_{mn}} |\psi_{mn}\rangle \tag{B.26}$$

where the indices $m, n \in \{2, \perp\}$ indicate whether the state is in the subspace containing the 2×2 or 1×1 blocks in $\mathcal{H}_\mathrm{A}$ and $\mathcal{H}_\mathrm{B}$. The expectation value of I_β splits accordingly as

$$I_\beta = \sum_{mn} p_{mn} I_\beta^{(mn)} \,. \tag{B.27}$$

In order to attain the quantum bound $I_\beta = 2\sqrt{2}\sqrt{1 + \beta^2/4}$ we must have $I_\beta^{(mn)} = 2\sqrt{2}\sqrt{1 + \beta^2/4}$ for each m, n for which $p_{mn} \neq 0$. However, except for $(m, n) = (2, 2)$, $I_\beta^{(mn)}$ is limited to the classical bound since the measurements on Alice's and/or Bob's side commute in the corresponding subspace. Thus, all of the support of $|\Psi\rangle$ must be in the subspace of $\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{B}$ containing the 2×2 blocks on both sides.

With respect to the 2×2 blocks, the state can be expressed as

$$|\Psi\rangle = \sum_{jk} \sqrt{q_{jk}} |\phi_{jk}\rangle |j\rangle |k\rangle \tag{B.28}$$

and the value of I_β, accordingly,

$$\begin{aligned} I_\beta &= \sum_{jk} q_{jk} \langle \phi_{jk} | \big(A_j (B_k + B'_k) + A'_j (B_k - B'_k) \big) | \phi_{jk} \rangle \,, \\ &= \sum_{jk} q_{jk} I_\beta^{(jk)} \,. \end{aligned} \tag{B.29}$$

Again, in order to attain the quantum bound, for each contribution (j, k) either we must have $I_\beta^{(jk)} = 2\sqrt{2}\sqrt{1 + \beta^2/4}$ or $q_{jk} = 0$. We can first get rid of the parts of Alice's and Bob's Hilbert spaces that don't contain $|\Psi\rangle$: if there are any js such that $q_{jk} = 0, \forall k$ or any ks such that $q_{jk} = 0, \forall j$ then we absorb the corresponding blocks $A_j \otimes |j\rangle\langle j|$ and $A'_j \otimes |j\rangle\langle j|$ or $B_k \otimes |k\rangle\langle k|$ and $B'_k \otimes |k\rangle\langle k|$ respectively into $A_\perp$ and $A'_\perp$ or $B_\perp$ and $B'_\perp$. For the remaining blocks, for each j there is at least one k and for each k at least one j such that $q_{jk} \neq 0$ and we must have $I_\beta^{(jk)} = 2\sqrt{2}\sqrt{1 + \beta^2/4}$. Following the remark at the end of the last subsection, there is a choice of bases in which, for all the remaining j and k,

$$A_j = Z \,, \qquad\qquad A'_j = X \,, \tag{B.30}$$

and

$$B_k + B'_k = 2\cos\bigl(\tfrac{\mu_\beta}{2}\bigr) Z \,, \tag{B.31}$$

$$B_k - B'_k = 2\sin\bigl(\tfrac{\mu_\beta}{2}\bigr) X \,. \tag{B.32}$$

This in turn implies $|\psi_{jk}\rangle = |\psi_\beta\rangle$ for all the remaining j, k for which $q_{jk} \neq 0$. We can also choose to set $|\psi_{jk}\rangle$ for the others since if $q_{jk} = 0$ then $\sqrt{q_{jk}}|\psi_{jk}\rangle = 0$ regardless of what $|\psi_{jk}\rangle$ is. We thus obtain that the state and measurements, in a suitable choice of the bases, are

$$|\Psi\rangle = |\psi_\beta\rangle \otimes |\mathrm{junk}\rangle \,, \tag{B.33}$$

with $|\mathrm{junk}\rangle = \sum_{jk} \sqrt{q_{jk}} |j\rangle|k\rangle$, and

$$A = Z \otimes \mathbb{I} \;\oplus\; A_\perp \,, \tag{B.34}$$

$$A' = X \otimes \mathbb{I} \;\oplus\; A'_\perp \,, \tag{B.35}$$

$$B = \Bigl(\cos\bigl(\tfrac{\mu_\beta}{2}\bigr) Z + \sin\bigl(\tfrac{\mu_\beta}{2}\bigr) X\Bigr) \otimes \mathbb{I} \;\oplus\; B_\perp \,, \tag{B.36}$$

$$B' = \Bigl(\cos\bigl(\tfrac{\mu_\beta}{2}\bigr) Z - \sin\bigl(\tfrac{\mu_\beta}{2}\bigr) X\Bigr) \otimes \mathbb{I} \;\oplus\; B'_\perp \,, \tag{B.37}$$

where only the first terms $(\ldots) \otimes \mathbb{I}$ act on the parts of $\mathcal{H}_\mathrm{A}$ and $\mathcal{H}_\mathrm{B}$ containing $|\Psi\rangle$.

Mixed states

The derivation up to this point easily adapts to allow for mixed states, since an arbitrary mixed state can be expressed as a convex sum

$$\rho = \sum_s p_s \Psi_s \tag{B.38}$$

of pure states. In order to attain the quantum bound for I_β, it must be attained with each pure state $|\Psi_s\rangle$. Following the reasoning of the previous subsection, we deduce that all the $|\Psi_s\rangle$ are in the subspace of $\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{B}$ containing the 2×2 measurement operator blocks and have the form

$$|\Psi_s\rangle = \sum_{jk} \sqrt{q^s_{jk}} |\phi^s_{jk}\rangle |j\rangle |k\rangle \,. \tag{B.39}$$

The only difference is that we only discard the blocks j for which $q^s_{jk} = 0, \forall k, s$ and k for which $q^s_{jk} = 0, \forall j, s$. We then obtain

$$|\Psi_s\rangle = |\psi_\beta\rangle \otimes |\mathrm{junk}_s\rangle \tag{B.40}$$

and, in turn,

$$\rho = \psi_\beta \otimes \sigma_\mathrm{junk} \,, \tag{B.41}$$

where σ_junk is a (not necessarily pure) state

$$\sigma_\mathrm{junk} = \sum_s p_s \, |\mathrm{junk}_s\rangle\langle\mathrm{junk}_s| \,. \tag{B.42}$$

General measurements

In general, measurements with only two outcomes can be expressed as convex sums of projective measurements. For the measurement operators we may write

$$A = \sum_j p_j A_j \,, \qquad A' = \sum_j p_j A'_j \,, \tag{B.43}$$

$$B = \sum_k q_k B_k \,, \qquad B' = \sum_k q_k B'_k \,, \tag{B.44}$$

with ${A_j}^2 = {A'_j}^2 = \mathbb{I}_\mathrm{A}$ and ${B_k}^2 = {B'_k}^2 = \mathbb{I}_\mathrm{B}$. I_β then decomposes as

$$I_\beta = \sum_{jk} p_j q_k \, I_\beta^{(jk)} \tag{B.45}$$

with

$$I_\beta^{(jk)} = \left\langle \beta A_j + A_j B_k + A_j B'_k + A'_j B_k - A'_j B'_k \right\rangle . \tag{B.46}$$

If the quantum bound is attained then all the $I_\beta^{(jk)}$s have to attain it individually. In particular, for $i = j = 1$, the results of the previous subsections imply that there is a choice of the bases in which the underlying state is

$$\rho = \psi_\beta \otimes \sigma_\mathrm{junk} \tag{B.47}$$

and

$$A_1 = Z \otimes \mathbb{I} \,\oplus\, A_\perp^{(1)}\,, \tag{B.48}$$
$$A_1' = X \otimes \mathbb{I} \,\oplus\, A'^{(1)}_\perp\,, \tag{B.49}$$
$$B_1 = \Big(\cos\big(\tfrac{\mu_\beta}{2}\big) Z + \sin\big(\tfrac{\mu_\beta}{2}\big) X\Big) \otimes \mathbb{I} \,\oplus\, B_\perp^{(1)}\,, \tag{B.50}$$
$$B_1' = \Big(\cos\big(\tfrac{\mu_\beta}{2}\big) Z - \sin\big(\tfrac{\mu_\beta}{2}\big) X\Big) \otimes \mathbb{I} \,\oplus\, B'^{(1)}_\perp\,. \tag{B.51}$$

Consider now $I_\beta^{(j1)}$ for $j \neq 1$. We can write it as

$$\begin{aligned} I_\beta^{(j1)} &= \big\langle A_j\big(\beta\mathbb{I} + B_1 + B_1'\big)\big\rangle + \big\langle A_j'\big(B_1 - B_1'\big)\big\rangle \\ &= \mathrm{Tr}\big[A_j\,(\tilde{\rho}_+ \otimes \sigma_{\mathrm{A}})\big] + \mathrm{Tr}\big[A_j'\,(\tilde{\rho}_- \otimes \sigma_{\mathrm{A}})\big] \end{aligned} \tag{B.52}$$

where

$$\tilde{\rho}_+ = \Big(\tfrac{\beta}{2} + \cos\big(\tfrac{\mu_\beta}{2}\big)\cos(\theta_\beta)\Big)\mathbb{I} + \Big(\tfrac{\beta}{2}\cos(\theta_\beta) + \cos\big(\tfrac{\mu_\beta}{2}\big)\Big) Z\,, \tag{B.53}$$
$$\tilde{\rho}_- = \sin\big(\tfrac{\mu_\beta}{2}\big)\sin(\theta_\beta) X\,, \tag{B.54}$$

and σ_{A} is the marginal of σ_{junk} on Alice's side. Using the relations (5.17) and (5.18) for θ_β and μ_β in terms of β (from the main text),

$$\tilde{\rho}_+ \otimes \sigma_{\mathrm{A}} = \frac{1}{2}\left[2\beta\,\mathbb{I} + \frac{\sqrt{2}\big(1 + 3\,\beta^2/4\big)}{\sqrt{1 + \beta^2/4}}\, Z\right] \otimes \sigma_{\mathrm{A}}\,, \tag{B.55}$$
$$\tilde{\rho}_- \otimes \sigma_{\mathrm{A}} = \frac{1}{2}\frac{\sqrt{2}\big(1 - \beta^2/4\big)}{\sqrt{1 + \beta^2/4}}\, X \otimes \sigma_{\mathrm{A}}\,. \tag{B.56}$$

In order for the traces in (B.52) to reach their maximal values, A_j and A_j' must be diagonal in the same bases as the operators $\tilde{\rho}_+ \otimes \sigma_{\mathrm{A}}$ and $\tilde{\rho}_- \otimes \sigma_{\mathrm{A}}$ that they are multiplied with. Note that $\tilde{\rho}_+$ in (B.55) has a negative eigenvalue for $\beta < 2$; a little algebra shows that

$$\frac{\sqrt{2}\big(1 + 3\,\beta^2/4\big)}{\sqrt{1 + \beta^2}} > 2\beta \tag{B.57}$$

rearranges to and is implied by $(1 - \beta^2/4)^2 > 0$. We can thus infer that

$$A_j = Z \otimes \mathbb{I} \,\oplus\, A_\perp^{(j)}\,, \qquad\qquad A_j' = X \otimes \mathbb{I} \,\oplus\, A'^{(j)}_\perp \tag{B.58}$$

for all j, and that A and A' have the form

$$A = Z \otimes \mathbb{I} \,\oplus\, A_\perp\,, \qquad\qquad A' = X \otimes \mathbb{I} \,\oplus\, A'_\perp \tag{B.59}$$

where $A_\perp = \sum_j p_j A_\perp^{(j)}$ and $A'_\perp = \sum_j p_j A'^{(j)}_\perp$ are bounded between $-\mathbb{I}$ and $\mathbb{I}$.

Applying the same approach to $I_\beta^{(1k)}$ for $k \neq 1$ we can similarly deduce that

$$B = \Big(\cos\big(\tfrac{\mu_\beta}{2}\big) Z + \sin\big(\tfrac{\mu_\beta}{2}\big) X\Big) \otimes \mathbb{I} \,\oplus\, B_\perp\,, \tag{B.60}$$

$$B' = \Big(\cos\big(\tfrac{\mu_\beta}{2}\big) Z - \sin\big(\tfrac{\mu_\beta}{2}\big) X\Big) \otimes \mathbb{I} \,\oplus\, B'_\perp \tag{B.61}$$

with $B_\perp = \sum_k q_k B_\perp^{(k)}$ and $B'_\perp = \sum_k q_k B'^{(k)}_\perp$.

This concludes our proof of Lemma 5.1 for progressively more general cases.

Bibliography

[ABB$^+$17] O. Andersson, P. Badziag, I. Bengtsson, I. Dumitru, and A. Cabello. Self-testing properties of Gisin's Elegant Bell inequality. *Phys. Rev. A*, 96:032119, 2017.

[ABG$^+$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.

[ADGL02] A. Acín, T. Durt, N. Gisin, and J. I. Latorre. Quantum nonlocality in two three-level systems. *Phys. Rev. A*, 65:052325, 2002.

[ADR82] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, 1982.

[AFDF$^+$18] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications*, 9(1):459, 2018.

[AGCA12] L. Aolita, R. Gallego, A. Cabello, and A. Acín. Fully nonlocal, monogamous, and random genuinely multipartite quantum correlations. *Phys. Rev. Lett.*, 108:100401, 2012.

[AGG05] A. Acín, R. Gill, and N. Gisin. Optimal Bell tests do not require maximally entangled states. *Phys. Rev. Lett.*, 95:210402, 2005.

[ALM$^+$11] M. Agnew, J. Leach, M. McLaren, F. S. Roux, and R. W. Boyd. Tomography of the quantum state of photons entangled in high dimensions. *Phys. Rev. A*, 84:062101, 2011.

[AM16] A. Acín and L. Masanes. Certified randomness in quantum physics. *Nature*, 540:213, 2016.

[AMP12] A. Acín, S. Massar, and S. Pironio. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.*, 108:100402, 2012.

[ApS17] MOSEK ApS. *The MOSEK optimization toolbox for MATLAB manual. Version 8.1.*, 2017.

[ApS18] MOSEK ApS. *The MOSEK Optimization Suite. Version 8.1.*, 2018.

[APVW16] A. Acín, S. Pironio, T. Vértesi, and P. Wittek. Optimal randomness certification from one entangled bit. *Phys. Rev. A*, 93:040102, 2016.

[Asp04] A. Aspect. *Introduction : John Bell and the second quantum revolution*, pages xvii – xxxix. Cambridge University Press, second edition, 2004.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[BBB$^+$12] J.-D. Bancal, C. Branciard, N. Brunner, N. Gisin, and Y.-C. Liang. A framework for the study of symmetric full-correlation Bell-like inequalities. *Journal of Physics A: Mathematical and Theoretical*, 45(12):125301, 2012.

[BC90] S. L. Braunstein and C. M. Caves. Wringing out better Bell inequalities. *Annals of Physics*, 202(1):22 – 56, 1990.

[BCP$^+$14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:839–840, 2014.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195, 1964.

[BFK09] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '09, pages 517–526, Washington, DC, USA, 2009. IEEE Computer Society.

[BGLP11] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio. Device-independent witnesses of genuine multipartite entanglement. *Phys. Rev. Lett.*, 106:250404, 2011.

[BKG$^+$18] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, 556(7700):223–226, 2018.

[BKP06] J. Barrett, A. Kent, and S. Pironio. Maximally nonlocal and monogamous quantum correlations. *Phys. Rev. Lett.*, 97:170409, 2006.

[BNS$^+$15] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang. Physical characterization of quantum devices from nonlocal correlations. *Phys. Rev. A*, 91:022115, 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.

[Bru02] D. Bruß. Characterizing entanglement. *Journal of Mathematical Physics*, 43(9):4237–4251, 2002.

[BŠCA18a] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín. Device-independent entanglement certification of all entangled states. *Phys. Rev. Lett.*, 121:180503, 2018.

[BŠCA18b] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín. Self-testing of Pauli observables for device-independent entanglement certification. *Phys. Rev. A*, 98:042336, 2018.

[BSS14] J.-D. Bancal, L. Sheridan, and V. Scarani. More randomness from the same data. *New Journal of Physics*, 16(3):033011, 2014.

[BST16] D. Bonneau, J. W. Silverstone, and M. G. Thompson. *Silicon quantum photonics*, pages 41–82. Springer-Verlag Berlin Heidelberg, 2016.

[BV04] S. Boyd and L. Vandenberghe. *Convex Optimization.* Cambridge University Press, 2004.

[CGL$^+$02] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88:040404, 2002.

[CGS17] A. Coladangelo, K. T. Goh, and V. Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8:15485, 2017.

[CHM$^+$16] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley. Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465, 2016.

[CHS$^+$15] J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing. Universal linear optics. *Science*, 349(6249):711–716, 2015.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[Cir80] B. S. Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4:93–100, 1980.

[CJA$^+$17] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín. Unbounded randomness certification using sequences of measurements. *Phys. Rev. A*, 95:020102, 2017.

[CK78] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[CK11] R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[CMA$^+$13] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.*, 111:130406, 2013.

[Col06] R. Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation.* PhD thesis, University of Cambridge, 2006.

[COP$^+$16] M. A. Ciampini, A. Orieux, S. Paesani, F. Sciarrino, G. Corrielli, A. Crespi, R. Ramponi, R. Osellame, and P. Mataloni. Path-polarization hyperentangled and cluster states of photons on a chip. *Light: Science &Amp; Applications*, 5:e16064, 2016.

[DEBZ10] T. Durt, B.-G. Englert, I. Bengtsson, and K. Zyczkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 08(04):535–640, 2010.

[dlT15] G. de la Torre. *From Quantum Foundations to Quantum Information Protocols and back.* PhD thesis, Universitat Politécnica de Catalunya - Institut de Ciéncies Fotóniques, 2015.

[DPA13] C. Dhara, G. Prettico, and A. Acín. Maximal quantum randomness in Bell tests. *Phys. Rev. A*, 88:052116, 2013.

[DPVR12] A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41:915–940, 2012.

[dV15] J. I. de Vicente. Simple conditions constraining the set of quantum correlations. *Phys. Rev. A*, 92:032103, 2015.

[dVSK13] J. I. de Vicente, C. Spee, and B. Kraus. Maximally entangled set of multipartite quantum states. *Phys. Rev. Lett.*, 111:110502, 2013.

[DW05] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[FC72] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28:938–941, 1972.

[FFW11] T. Franz, F. Furrer, and R. F. Werner. Extremal quantum correlations and cryptographic security. *Phys. Rev. Lett.*, 106:250502, 2011.

[Fin82] A. Fine. Hidden variables, joint probability, and the Bell inequalities. *Phys. Rev. Lett.*, 48:291–295, 1982.

[Fro81] M. Froissart. Constructive generalization of Bell's inequalities. *Il Nuovo Cimento B*, 64:241–251, 1981.

[FSA$^+$13] T. Fritz, A.B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín. Information causality as a physical principle. *Nature Communications*, 4:2263, 2013.

[Gam] Gaming labs - random number generator. https://www.gaminglabs.com/random-number-generator-rng. Accessed: 2018-10-02.

[Gen03] J. E. Gentle. *Random Number Generation and Monte Carlo Methods*. Springer, New York, NY, USA, 2nd edition, 2003.

[GHZ89] D.M. Greenberger, M.A. Horne, and A. Zeilinger. *Going Beyond Bell's Theorem*, volume 37, pages 69 – 72. Springer, Dordrecht, 1989.

[Gis09] N. Gisin. *Bell Inequalities: Many Questions, a Few Answers*, volume 73, pages 125 – 138. Springer, Dordrecht, 2009.

[GK04] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, 2004.

[GKW$^+$18] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani. Geometry of the set of quantum correlations. *Phys. Rev. A*, 97:022104, 2018.

[GMG$^+$18] S. Gómez, A. Mattar, E. S. Gómez, D. Cavalcanti, O. Jiménez Farías, A. Acín, and G. Lima. Experimental nonlocality-based randomness generation with nonprojective measurements. *Phys. Rev. A*, 97:040102, 2018.

[Goo] Google AI - Quantum AI publications database. https://ai.google/research/pubs?area=QuantumAI. Accessed: 2018-11-13.

[GT09] O. Gühne and G. Tóth. Entanglement detection. *Physics Reports*, 474(1):1 – 75, 2009.

[GVW$^+$15] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, 2015.

[HBD$^+$15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:682, 2015.

[HP13] M. Huber and M. Pawłowski. Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement. *Phys. Rev. A*, 88:032309, 2013.

[HSP$^+$17] N. C. Harris, G. R. Steinbrecher, M. Prabhu, Y. Lahini, J. Mower, D. Bunandar, C. Chen, F. N. C. Wong, T. Baehr-Jones, M. Hochberg, S. Lloyd, and D. Englund. Quantum transport simulations in a programmable nanophotonic processor. *Nature Photonics*, 11:447, 2017.

[IBM] IBM Research Blog - Quantum computing. https://www.ibm.com/blogs/research/category/quantcomp/. Accessed: 2018-11-13.

[IDQ] ID Quantique - Random Numbers. https://www.idquantique.com/random-number-generation/overview/. Accessed: 2018-10-02.

[JAW$^+$00] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4):1675–1680, 2000.

[JLL$^+$08] S.-W. Ji, J. Lee, J. Lim, K. Nagata, and H.-W. Lee. Multisetting Bell inequality for qudits. *Phys. Rev. A*, 78:052103, 2008.

[Kan16] J. Kaniewski. Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt 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.

[KGZ$^+$00] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski, and A. Zeilinger. Violations of local realism by two entangled N-dimensional systems are stronger than for two qubits. *Phys. Rev. Lett.*, 85:4418–4421, 2000.

[KHLZ17] M. Krenn, A. Hochrainer, M. Lahiri, and A. Zeilinger. Entanglement by path identity. *Phys. Rev. Lett.*, 118:080401, 2017.

[KRR$^+$17] M. Kues, C. Reimer, P. Roztocki, L. R. Cortés, S. Sciara, B. Wetzel, Y. Zhang, A. Cino, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, J. Azaña, and R. Morandotti. On-chip generation of high-dimensional entangled quantum states and their coherent control. *Nature*, 546:622, 2017.

[LCL07] S.-W. Lee, Y. W. Cheong, and J. Lee. Generalized structure of Bell inequalities for bipartite arbitrary-dimensional systems. *Phys. Rev. A*, 76:032108, 2007.

[LLD09] Y.-C. Liang, C.-W. Lim, and D.-L. Deng. Reexamination of a multisetting Bell inequality for qudits. *Phys. Rev. A*, 80:052116, 2009.

[Lof04] J. Lofberg. YALMIP : a toolbox for modeling and optimization in MATLAB. In *2004 IEEE International Conference on Robotics and Automation (IEEE Cat. No.04CH37508)*, pages 284–289, 2004.

[LRY$^+$10] J. Lim, J. Ryu, S. Yoo, C. Lee, J. Bang, and J. Lee. Genuinely high-dimensional nonlocality optimized by complementary measurements. *New Journal of Physics*, 12(10):103012, 2010.

[LYL$^+$17] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics*, 11:509, 2017.

[MA16] A. Máttar and A. Acín. Implementations for device-independent quantum key distribution. *Physica Scripta*, 91(4):043003, 2016.

[McK14] M. McKague. Self-testing graph states. In *Revised Selected Papers of the 6th Conference on Theory of Quantum Computation, Communication, and Cryptography - Volume 6745*, TQC 2011, pages 104–120, New York, NY, USA, 2014. Springer-Verlag New York, Inc.

[Mic] Microsoft Quantum. https://www.microsoft.com/en-us/quantum/. Accessed: 2018-11-13.

[MM11] M. McKague and M. Mosca. Generalized self-testing and the security of the 6-state protocol. In *Proceedings of the 5th Conference on Theory of Quantum Computation, Communication, and Cryptography*, TQC'10, pages 113–130, Berlin, Heidelberg, 2011. Springer-Verlag.

[MN98] M. Matsumoto and T. Nishimura. Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model. Comput. Simul.*, 8(1):3–30, 1998.

[MPA11] L. Masanes, S. Pironio, and A. Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2:238, 2011.

[MS13] C. A. Miller and Y. Shi. Optimal Robust Self-Testing by Binary Nonlocal XOR Games. In S. Severini and F. Brandao, editors, *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*, volume 22 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 254–262, Dagstuhl, Germany, 2013. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[MY04] D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, 2004.

[MYS12] M. McKague, T.H. Yang, and V. Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[NC11] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[NGHA15] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín. Information causality as a physical principle. *Nature Communications*, 6:6288, 2015.

[NPA07] M. Navascués, S. Pironio, and A. Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, 2007.

[NPA08] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.

[NSBSP18] O. Nieto-Silleras, C. Bamps, J. Silman, and S. Pironio. Device-independent randomness generation from several Bell estimators. *New Journal of Physics*, 20(2):023049, 2018.

[NSPS14] O. Nieto-Silleras, S. Pironio, and J. Silman. Using complete measurement statistics for optimal device-independent randomness evaluation. *New Journal of Physics*, 16(1):013035, 2014.

[NW10] M. Navascués and H. Wunderlich. A glance beyond the quantum model. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 466(2115):881–890, 2010.

[OPSV13] J. O'Brien, B. Patton, M. Sasaki, and J. Vučković. Focus on integrated quantum optics. *New Journal of Physics*, 15(3):035016, 2013.

[PAB$^+$09] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[PAM$^+$10] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–4, 2010.

[Pea70] P. M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, 1970.

[PGS$^+$17] S. Paesani, A. A. Gentile, R. Santagati, J. Wang, N. Wiebe, D. P. Tew, J. L. O'Brien, and M. G. Thompson. Experimental Bayesian quantum phase estimation on a silicon photonic chip. *Phys. Rev. Lett.*, 118:100503, 2017.

[Pic18] Picos. *A Python Interface to Conic Optimization Solvers*, 2018.

[PM13] S. Pironio and S. Massar. Security of practical private randomness generation. *Phys. Rev. A*, 87:012336, 2013.

[PNA10] S. Pironio, M. Navascués, and A. Acín. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM J. on Optimization*, 20(5):2157–2180, 2010.

[PPK+09] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski. Information causality as a physical principle. *Nature*, 461:1101–1104, 2009.

[PR94] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24:379–385, 1994.

[PVN14] K. F. Pál, T. Vértesi, and M. Navascués. Device-independent tomography of multipartite quantum states. *Phys. Rev. A*, 90:042340, 2014.

[Qui] Quintessence labs. https://www.quintessencelabs.com/. Accessed: 2018-11-13.

[Ren05] R. Renner. *Security of Quantum Key Distribution.* PhD thesis, ETH Zurich, 2005.

[Rol15] R. Rolland. *Randomness in Cryptography*, pages 451–459. Springer International Publishing, Cham, 2015.

[RTHH16] R. Ramanathan, J. Tuziemski, M. Horodecki, and P. Horodecki. No quantum realization of extremal no-signaling boxes. *Phys. Rev. Lett.*, 117:050401, 2016.

[RUV13] B. W. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496:456, 2013.

[RZBB94] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, 1994.

[SA18] J. Sturm and AdvOL. SeDuMi : Optimization over symmetric cones, 2018. http://sedumi.ie.lehigh.edu/.

[ŠASA16] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín. Self-testing protocols based on the chained Bell inequalities. *New Journal of Physics*, 18(3):035013, 2016.

[SAT+17] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.*, 119:040402, 2017.

[SBO$^+$13] J. W. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, V. Zwiller, G. D. Marshall, J. G. Rarity, J. L. O'Brien, and M. G. Thompson. On-chip quantum interference between silicon photon-pair sources. *Nature Photonics*, 8:104, 2013.

[ŠCAA18] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín. Self-testing multipartite entangled states through projections onto two systems. *New Journal of Physics*, 20(8):083041, 2018.

[SGG$^+$02] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug & play system. *New Journal of Physics*, 4(1):41, 2002.

[SLK06] W. Son, J. Lee, and M. S. Kim. Generic Bell inequalities for multipartite arbitrary dimensional systems. *Phys. Rev. Lett.*, 96:060406, 2006.

[SMSC$^+$15] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, 2015.

[SPL$^+$12] C. Schaeff, R. Polster, R. Lapkiewicz, R. Fickler, S. Ramelow, and A. Zeilinger. Scalable fiber integrated source for higher-dimensional path-entangled photonic qunits. *Opt. Express*, 20(15):16145–16153, 2012.

[SSC$^+$15] K. Schwaiger, D. Sauerwein, M. Cuquet, J. I. de Vicente, and B. Kraus. Operational multipartite entanglement measures. *Phys. Rev. Lett.*, 115:150502, 2015.

[STY$^+$13] J. Sun, E. Timurdogan, A. Yaacobi, E. S. Hosseini, and M. R. Watts. Large-scale nanophotonic phased array. *Nature*, 493:195, 2013.

[Sve87] G. Svetlichny. Distinguishing three-body from two-body nonseparability by a Bell-type inequality. *Phys. Rev. D*, 35:3066–3069, 1987.

[Tsi93] B. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8:329–345, 1993.

[VV14] U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, 2014.

[WBA18] E. Woodhead, B. Bourdoncle, and A. Acín. Randomness versus nonlocality in the Mermin-Bell experiment with three parties. *Quantum*, 2:82, 2018.

[WBV$^+$16] J. Wang, D. Bonneau, M. Villa, J. W. Silverstone, R. Santagati, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson. Chip-to-chip quantum photonic interconnect by path-polarization interconversion. *Optica*, 3(4):407–413, 2016.

[WCY$^+$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.

[Weh06] S. Wehner. Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. *Phys. Rev. A*, 73:022110, 2006.

[Wit15] P. Wittek. Algorithm 950: Ncpol2sdpa – sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables. *ACM Trans. Math. Softw.*, 41(3):21:1–21:12, 2015.

[WKB$^+$19] E. Woodhead, J. Kaniewski, B. Bourdoncle, A. Salavrakos, J. Bowles, R. Augusiak, and A. Acín. Maximal randomness from partially entangled states. *arXiv:1901.06912*, 2019.

[Wol14] Wolfram. Mathematica 10.0, 2014.

[WPD$^+$18] J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson. Multidimensional quantum entanglement with large-scale integrated optics. *Science*, 360(6386):285–291, 2018.

[WPS$^+$17] J. Wang, S. Paesani, R. Santagati, S. Knauer, A. A. Gentile, N. Wiebe, M. Petruzzella, J. L. O'Brien, J. G. Rarity, A. Laing, and M. G. Thompson. Experimental quantum hamiltonian learning. *Nature Physics*, 13:551, 2017.

[YVB$^+$14] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués. Robust and versatile black-box certification of quantum devices. *Phys. Rev. Lett.*, 113:040401, 2014.

[ZG08] S. Zohren and R. D. Gill. Maximal violation of the Collins-Gisin-Linden-Massar-Popescu inequality for infinite dimensional states. *Phys. Rev. Lett.*, 100:120406, 2008.