PhD thesis

CERTIFICATION OF MANY-BODY SYSTEMS

17th May 2019

Thesis Supervisor
Prof. Dr. Antonio Acín

Candidate
Flavio Baccari

Abstract

Quantum physics is arguably both the most successful and the most counterintuitive physical theory of all times. Its extremely accurate predictions on the behaviour of microscopic particles have led to unprecedented technological advances in various fields and yet, many quantum phenomena defy our classical intuition.

Starting from the 1980's, however, a paradigm shift has gradually taken hold in the scientific community, consisting in studying quantum phenomena not as inexplicable conundrums but as useful resources. This shift marked the birth of the field of quantum information science, which has since then explored the advantages that quantum theory can bring to the way we process and transfer information.

By now, it is a very well established fact that encoding bits in quantum particles can lead for instance to more efficient computations as well as extremely secure communications. Because of its practical applications to every-day life, quantum information science has therefore attracted a lot of political and economic interest. Several initiatives have been recently launched with the purpose of bridging the gap between basic science and industry in this field, both at the national and the international level. At the same time, more and more companies are increasing their effort in producing quantum devices at the commercial level.

There is no doubt that we have entered the era of the near-term quantum devices, where controllable quantum systems composed of tens or hundreds of particles are becoming increasingly more accessible. In such a scenario, certifying that these devices are exhibiting their appealing quantum properties constitutes a timely problem. Importantly, for the desired certification methods to be applicable in realistic situations, they have to be scalable with the system size. In other words, they have to involve computational and experimental requirements that grow polynomially with the number of particles in the system of interest.

In this thesis, we introduce scalable certification tools that apply to various operational properties of many-body quantum systems. In the first three cases we consider, we base our certification protocols on the

detection of nonlocal correlations. These kinds of non-classical correlations that can displayed by quantum states allow one to assess relevant properties in a device-independent manner, that is, without assuming anything about the specific functioning of the device producing the state of interest or the implemented measurements.

In the first scenario we present an efficient method to detect multipartite entanglement in a device-independent way. We do so by introducing a numerical test for nonlocal correlations that involves computational and experimental resources that scale polynomially with the system number of particles. We show the range of applicability of the method by using it to detect entanglement in various families of multipartite systems.

In multipartite systems, however, it is often more informative to provide quantitative statements. We address this problem in the second scenario by introducing scalable methods to quantify the nonlocality depth of a multipartite systems, that is, the number of particles sharing nonlocal correlations among each other. We show how to do that by making use of the knowledge of two-body correlations only and we apply the resulting techniques to experimental data from a system of a few hundreds of atoms.

In the third scenario, we move to consider self-testing, which is the most informative certification method based on nonlocality. Indeed, in a self-testing task, one is interested in characterising the state of the system and the measurement performed on it, by simply looking at the resulting correlations. We introduce the first scalable self-testing method based on Bell inequalities and apply it to graph states, a well-known family of multipartite quantum states. Moreover, we show that the certification achieved with our method is robust against experimental imperfections.

Lastly, we address the problem of certifying the result of quantum optimizers. They are quantum devices designed to estimate the ground-state energy of classical spin systems. We provide a way to efficiently compute a convergent series of upper and lower bounds to the minimum of interest, which at each step allows one to certify the output of any quantum optimizer.

Resumen

La física cuántica es posiblemente la teoría física más exitosa y la más contraintuitiva jamás desarollada. A pesar de que sus predicciones extremadamente precisas sobre el comportamiento de las partículas microscópicas han llevado a avances tecnológicos sin precedentes en varios campos, muchos fenómenos cuánticos desafían nuestra intuición basada en una concepción clásica de la física.

Sin embargo, a partir de la década de 1980 tuvo lugar un cambio de paradigma en la comunidad científica, que se orientó en estudiar los fenómenos cuánticos no como enigmas inexplicables, sino como recursos útiles. Este cambio marcó el nacimiento del campo de la ciencia de la información cuántica, que desde entonces ha explorado las ventajas que la teoría cuántica puede aportar a la forma en que procesamos y transferimos la información.

Hoy en día es un hecho bien establecido que la codificación de información en partículas cuánticas puede llevar, por ejemplo, a procesos de cálculo más eficientes, así como a comunicaciones extremadamente seguras. Además, debido a sus aplicaciones prácticas a la vida cotidiana, la ciencia de la información cuántica ha atraído un gran interés político y económico. Recientemente se han lanzado varias iniciativas con el propósito de cerrar la brecha entre la ciencia básica y la industria en este campo, tanto a nivel nacional como internacional. Al mismo tiempo, cada vez más empresas están incrementando sus esfuerzos para producir dispositivos cuánticos a nivel comercial.

No hay duda de que hemos entrado en la era de la primera generación de dispositivos cuánticos, en la cual los sistemas cuánticos controlables compuestos de decenas o cientos de partículas son cada vez más accesibles. En tal escenario, el certificar que estos dispositivos exhiben sus atractivas propiedades cuánticas constituye un problema fundamental. Es importante destacar que, para que los métodos de certificación deseados sean aplicables en situaciones reales, éstos deben ser escalables con el tamaño del sistema. En otras palabras, tienen que basarse en requerimientos computacionales y experimentales que crezcan, a lo sumo,polinomialmente

con el número de partículas en el sistema de interés.

En esta tesis, introducimos herramientas de certificación escalables que se aplican a varias propiedades operativas de sistemas cuánticos de muchos cuerpos. En los primeros tres casos que consideramos, basamos nuestros protocolos de certificación en la detección de correlaciones no locales. Estos tipos de correlaciones no clásicas, que únicamente pueden ser producidas por sistemas cuánticos, permiten evaluar propiedades relevantes de forma independiente del dispositivo, es decir, sin realizar hipótesis acerca del funcionamiento específico del dispositivo que produce el estado de interés o las mediciones implementadas.

En el primer escenario, presentamos un método eficiente para detectar entrelazamiento en sistemas multipartitos de forma independiente del dispositivo. Lo hacemos mediante la introducción de una prueba numérica para las correlaciones no locales que involucra recursos computacionales y experimentales que escalan polinomialmente con el número de partículas del sistema. Mostramos el rango de aplicabilidad de dicho método usándolo para detectar entrelazamiento en varias familias de sistemas multipartitos.

Sin embargo, al tratar con sistemas de muchos cuerpos a menudo es más informativo proporcionar informaciones cuantitativas. Abordamos este problema en el segundo escenario mediante la introducción de métodos escalables para cuantificar la profundidad no local (non-locality depth) de un sistema multipartito, es decir, la cantidad de partículas que comparten correlaciones no locales entre sí. Mostramos cómo realizar dicha cuantificación a partir del conocimiento únicamente de los correladores de dos cuerpos, y aplicamos las técnicas resultantes a los datos experimentales de un sistema de unos pocos cientos de átomos.

En el tercer escenario, pasamos a considerar el caso de self-testing, que es el método de certificación más informativo basado en la no localidad. De hecho, en una tarea de self-testing, el objetivo es caracterizar el estado del sistema y las mediciones realizadas en él, simplemente observando las correlaciones resultantes. Introducimos el primer método de self-testing escalable basado en las desigualdades de Bell y lo aplicamos a estados de grafo, una familia muy conocida de estados cuánticos multipartitos. Además, demostramos que la certificación lograda con nuestro método es robusta a imperfecciones experimentales.

Por último, consideramos el problema de certificar el resultado de optimizadores cuánticos. Estos son dispositivos cuánticos diseñados para estimar la energía del estado fundamental de sistemas de espines clásicos. Desarollamos un método eficiente para calcular una serie convergente de límites superiores e inferiores al mínimo de interés, que en cada paso permite certificar el resultado de cualquier optimizador cuántico.

Resum

La física quàntica és, sens dubte, la teoria física més reeixida i més contra-intuïtiva de tots els temps. Les seves prediccions extremadament precises sobre el comportament de les partícules microscòpiques han donat lloc a avenços tecnològics sense precedents en diversos camps i, no obstant això, molts fenòmens quàntics desafien la nostra intuïció clàssica.

A partir de la dècada dels 80, però, un canvi de paradigma s'ha anat establint entre la comunitat científica, consistint a estudiar fenòmens quàntics no tan com quelcom inexplicable o contra-intuïtiu, sinó com a recursos útils per a certes tasques. Aquest canvi va marcar el naixement del camp de la ciència de la informació quàntica, que des de llavors ha explorat els avantatges que la teoria quàntica pot aportar a la nostra manera de processar i transferir informació.

Avui dia és un fet molt ben establert que la codificació de bits en les partícules quàntiques pot conduir, per exemple, a càlculs més eficients, així com a comunicacions extremadament segures. A causa de les seves aplicacions pràctiques a la vida quotidiana, la ciència de la informació quàntica ha atret molt interès polític i econòmic. Recentment s'han posat en marxa diverses iniciatives amb la finalitat de reduir la distància entre la ciència bàsica i la indústria en aquest camp, tant a nivell nacional com internacional. Al mateix temps, cada vegada són més les empreses que estan duent a terme esforços en la producció de dispositius quàntics a nivell comercial.

No hi ha dubte que hem entrat a l'era dels dispositius quàntics a curt termini, on els sistemes quàntics controlables composts per desenes o centenars de partícules són cada vegada més accessibles. En aquest escenari, la certificació que aquests dispositius satisfan, en efecte, les seves atractives propietats quàntiques constitueix un problema oportú i altament rellevant. És important destacar que per tal que els mètodes de certificació desitjats siguin aplicables a situacions realistes, han de ser escalables amb la mida del sistema. En altres paraules, han complir amb els requisits computacionals i experimentals que demanen un creixement polinomial amb el nombre de partícules del sistema d'interès.

En aquesta tesi, introduïm eines de certificació escalables que s'apliquen a diverses propietats operacionals dels sistemes quàntics de molts cossos. En els tres primers casos que considerem, basem els nostres protocols de certificació en la detecció de correlacions no locals. Aquests tipus de correlacions no clàssiques, que es poden revelar per alguns estats quàntics, permeten avaluar les propietats pertinents d'una manera independent del dispositiu, és a dir, sense assumir cap hipòtesi sobre el funcionament específic del dispositiu que produeix l'estat d'interès o les mesures implementades.

En el primer escenari presentem un mètode eficaç per detectar l'entrellaçament de múltiples sistemes de manera independent del dispositiu. Ho fem introduint una prova numèrica per a correlacions no locals que impliqui recursos computacionals i experimentals que escala polinomialment amb el nombre de partícules del sistema. Mostrem el rang d'aplicabilitat del mètode utilitzant-lo per detectar l'entrellaçament en diverses famílies de sistemes multipartits.

En sistemes multipartits, però, sovint és més informatiu proporcionar declaracions quantitatives. Abordem aquest problema en el segon escenari introduint mètodes escalables per quantificar la profunditat de no localitat d'un sistema multipartit, és a dir, el nombre de partícules que comparteixen correlacions no locals entre elles. Mostrem com fer-ho fent ús del coneixement de les correlacions de dos cossos i apliquem les tècniques resultants a dades experimentals a partir d'un sistema d'uns quants centenars d'àtoms.

En el tercer escenari, considerem l'anomenat self-testing (autoavaluació), que és el mètode de certificació més informatiu basat en la no localitat. De fet, en una tasca de self-testing, interessa caracteritzar l'estat del sistema i es mesures que s'hi fan, només a partir de les correlacions resultants. Introduïm el primer mètode de self-testing escalable basat en les desigualtats de Bell i l'aplicem als estats de grafs, una coneguda família d'estats quàntics multipartits. A més, demostrem que la certificació aconseguida amb el nostre mètode és robusta contra imperfeccions experimentals.

Finalment, abordem el problema de certificar el resultat dels optimitzadors quàntics. Són dispositius quàntics dissenyats per preparar una aproximació de l'estat de menor energia en els sistemes de spin clàssics. Proporcionem un mètode per calcular de manera eficient unes seqüències convergents de fites superiors i inferiors al mínim d'interès, i que a cada pas ens permet certificar la sortida de qualsevol optimitzador quàntic.

Contents

List of publications

- F. Baccari, D. Cavalcanti, P. Wittek, A. Acín, "Efficient device-independent entanglement detection for multipartite systems", Physical Review X 7, 021042 (2017)

- F. Baccari, J. Tura, M. Fadel, A. Aloy, J.-D. Bancal, N. Sangouard, M. Lewenstein, A. Acín, R. Augusiak, "Bell correlations depth in many-body systems", arXiv:1802.09516 (2018)

- F. Baccari, C. Gogolin, P. Wittek, A. Acín, "Verification of Quantum Optimizers", arXiv:1808.01275 (2018)

- F. Baccari, R. Augusiak, I. Šupić, J. Tura, A. Acín, "Scalable Bell inequalities for qubit graph states and robust self-testing", arXiv:1812.10428 (2018)

Publications and preprints relevant to the thesis, but not forming part of it

- M. Arias, G. Canas, E. S. Gomez, J. F. Barra, G. B. Xavier, G. Lima, V. D'Ambrosio, F. Baccari, F. Sciarrino, A. Cabello, "Testing noncontextuality inequalities that are building blocks of quantum correlations", Physical Review A 92, 032126 (2015)

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

- A. Aloy, J. Tura, F. Baccari, A. Acín, M. Lewenstein, R. Augusiak, "Device-Independent Witnesses of Entanglement Depth from two-body correlators", arXiv:1807.06027 (2018)

- J. Tura, A. Aloy, F. Baccari, A. Acín, M. Lewenstein, R. Augusiak, "Optimization of device-independent witnesses of entanglement depth from two-body correlators", arXiv:1903.09533 (2019)

List of acronyms

LP	Linear programming
SDP	Semidefinite programming
LOCC	Local operations and classical communication
PPT	Positive partial transpose
GME	Genuine multipartite entanglement
GHZ	Greenberger-Horne-Zeilinger
EPR	Einstein-Podolski-Rosen
POVM	Positive operator-valued measure
LHV	Local hidden variable
NPA	Navascués-Pironio-Acín
GMNL	Genuinely multipartite nonlocal
CHSH	Clauser-Horne-Shimony-Holt
BB	Branch-and-bound
CBB	Chordal branch-and-bound

Chapter 1

Introduction

We give a brief introduction to the field of quantum information theory and to the notion of device-independent protocols. Afterwards, we present the general motivation behind this work and we summarise our main contributions.

1.1 Introduction to quantum information theory

At the beginning of the 20th century, the formulation of quantum theory constituted a complete change of paradigm in how physics described the world. The many counterintuitive phenomena that govern the behaviour of quantum particles have long since represented a puzzle for all scientists. Nevertheless, quantum mechanics is arguably the most successful physical theory of all times, having been capable to predict extremely accurately many new phenomena and leading to unprecedented scientific advances, especially in the study of matter and particle physics.

In more recent times, the ability to control and manipulate single quantum particles, initiated by the advancements in quantum optics, started a second wave of studies on the fundamental properties of quantum theory. While allowing one to analyse more closely the paradoxical effects predicted by the superposition principle and measurement postulates, the new experiments also stimulated a change of perspective that proposed to look at the paradoxical properties of quantum systems as resources.

Taking from the expanding field of information theory, the idea that started forming was that encoding bits into quantum particles could bring advantages in the way the information is processed and transferred. The consecutive seminal works of Weisner, Bennett and Brassard introduced the first quantum cryptography [BB84] and quantum coding [BW92] pro-

tocols and opened the door to many more, including the first algorithms for quantum computers. After nearly 40 years of research, quantum information science is currently a well-established field, whose interests range in directions as diverse as optimisation problems, secure communication and chemistry [NC02].

In this thesis we focus on a particular framework for quantum information protocols: the device-independent scenario. Such a framework originated from the foundational studies of John Bell in the 1960's, who was the first to discover that composite quantum systems can exhibit correlations that escape any classical explanation [Bel64]. Further studies showed that these correlations, referred to as nonlocal, allow one to infer properties of the system in a device-independent manner, that is, without making assumptions about the devices that produce and manipulate it [BCP$^+$14].

1.2 Motivation and main contributions

The last years have witnessed a serious increase in political, scientific and economic interest towards bridging the gap between industry and research in quantum information theory. In fact, apart from keeping the impulse of basic science, the field is rapidly advancing in more applicative directions. This tendency is evident if one looks at the number of new quantum-inspired start-ups that have been launched in the last two years only. Quantum technologies have also attracted the interest of the big tech companies all over the world: each of them, ranging from Google, IBM, Amazon to Alibaba, has started developing its own prototype of quantum computer.

Indeed, quantum computing and quantum simulation constitute two of the most promising research directions that could find commercial applications in the near future. Their focus is on harnessing properties of large quantum states in order to solve problems that no classical computer can tackle, one prominent examples being the simulation of composite quantum systems themselves. Being able to perform calculations at such an unprecedented level of complexity opens the way to potential breakthroughs in fields as diverse as finance, chemistry, medicine and machine learning.

For all of these advances to be possible, a compelling requirement is not only to produce and control larger and larger quantum systems, but also to be able to verify that these systems are exhibiting the features that make them appealing in the first place. In other words, the ubiquitous problem that these quantum technologies are facing is that of certifying

whether a given many-body quantum system satisfies some operational properties. Among others, the crucial questions are: is this given system in an entangled state? Does the observed state correspond to the ground state of a given hamiltonian? Does it contain the solution to a hard classical optimisation problem?

To be of practical use, the desired certification methods should be scalable in the systems size. More precisely, if one is interested in detecting relevant properties of many-body states, any approach that requires collecting and processing an amount of information that grows exponentially with the system size is bound to become intractable for large enough systems. The main goal of this thesis is to provide scalable certification techniques for some of the most significant operational properties of quantum many-body systems. In most of the scenarios we consider, we adopt a device-independent framework, which is particularly appealing because it allows one to assess these properties by making no assumption on the internal working of the quantum device under study.

1.2.1 Device-independent multipartite entanglement detection

Entanglement is provably a vital ingredient for many of the most relevant protocols in quantum information theory. For this reason, certifying that a given multi-particle system is entangled is a crucial step for the practical implementation of these protocols [GT09]. From the theoretical point of view, it is well known that determining whether a given quantum state is not separable is a hard problem. Therefore, there is no hope to find an efficient criterion that can determine whether any density matrix is entangled or not. Despite the complexity obstacle, the practical interest of the problem has obviously stimulated a lot of research on approximate entanglement detection methods.

Nevertheless, all the known techniques suffer from at least one of the following drawbacks: i) being tailored to a very specific class of states, hence lacking generality, or ii) requiring an amount of information on the system that scales exponentially with the number of particles, or iii) constituting an inefficient test from the computational point of view.

Contribution: We introduce a device-independent multipartite entanglement detection method that can be applied to any set of observed correlations and that meets all the experimental and computational scalability requirements. Indeed, it necessitates the knowledge of up to four-body correlations, which can be estimated by performing a polynomial amount of measurements. Moreover, the entanglement criterion can be cast into an efficient numerical test, consisting in solving a semidefinite

program involving a number of variables that scales polynomially with N. The price to pay is that the introduced technique is a relaxation of the nonlocality detection problem, hence it can only provide necessary conditions for non-separability. Nevertheless, we examine several scenarios and we provide examples of relevant classes of multipartite states whose entanglement is successfully detected by our method for systems of few tens of particles.

1.2.2 Detecting nonlocality depth with two-body correlators

Bell nonlocality has attracted an increasing amount of attention over the last years, not only for its fundamental interest, but also for its role in device-independent quantum information protocols [BCP$^+$14]. Remarkably, while nonlocal correlations have been extensively explored in the bipartite scenarios, their features in multipartite settings are much less characterised. The main reason for that is the exponentially increasing computational complexity of the multipartite scenario, which prevents one from having a complete understanding of the space of classical, quantum and even post-quantum correlations for an arbitrary number of parties.

An interesting solution to overcome these difficulties, first proposed in [TAS$^+$14], is to restrict the study to the problem of detecting nonlocal correlations with the knowledge of two-body correlations only. Surprisingly enough, by further imposing permutational symmetry on the quantities of interest, the characterisation of local correlations dramatically simplifies, allowing one to show that such a limited amount of information is enough to detect nonlocality in systems composed of any number of particles. Apart from a theoretical interest, the introduced framework also has a practical relevance, since these quantities can be estimated by means of collective measurements. This simplification led to the first experimental demonstration of Bell correlations in many-body systems composed of thousands of particles [SBA$^+$16, EKHK17].

So far, the above-mentioned techniques were able to provide qualitative information about the system, namely confirming the presence of nonlocal correlations. However, the most relevant statements in a multipartite setting are actually those of quantitative nature, such as the estimation of the so-called nonlocality depth, which represents the amount of particles genuinely sharing non-classical correlations in the state. Compared to the case of entanglement, in the field of nonlocality this direction remains almost unexplored, mainly due to the lack of efficient methods that can estimate nonlocality depth.

Contribution: We address the question of detecting nonlocality depth in a multipartite scenario with the knowledge of the symmetrised two-body correlations only. To do so, we introduce a general framework and we show that, for any value of nonlocality depth, the complexity of the problem is polynomial in the number of particles. This allows us to obtain a complete characterisation of Bell inequalities detecting values of nonlocality depth $k \leq 6$, for the scenarios with a number of particles $N \leq 15$. Moreover, we show that those values of nonlocality depth can be detected and distinguished for any N. Lastly, we study the use of our techniques to many-body systems and we apply them to experimental data from a Bose-Einstein condensate.

1.2.3 Scalable self-testing from Bell inequalities

Self-testing is the strongest form of device-independent verification of a quantum device [MY04]. By simply exploiting the information encoded in the correlations produced by a system, a self-testing protocol allows one to certify the quantum state that was produced and the local measurements that were performed on it. Such a tool is particularly interesting because it offers a way to guarantee that a quantum device is working properly without the need of knowing its internal functioning.

In recent years, many self-testing protocols have been proposed, tailored to various families of bipartite and multipartite quantum states. The considered approaches generally differ from each other depending on the amount of information they require. The simplest method introduced so far is based on Bell inequalities, providing a self-testing statement that relies solely on the fact that the observed correlations achieve the maximal quantum violation of a given Bell inequality.

Another feature of a self-testing protocol that is relevant for practical applications is its scalability. Indeed, if one is interested in certifying properties of multipartite states, any approach based on an exponentially scaling amount of information is bound to become intractable for large enough systems. To the best of our knowledge, no polynomial Bell-inequality-based self-testing method has been introduced so far.

Contribution: We present the first scalable self-testing technique based on the maximal violation of Bell inequalities. To do so, we focus on the well-known graph states, a family of multipartite quantum states that have shown to be relevant for many quantum information protocols. Given a graph state, we are able to derive a Bell inequality maximally violated by it and we are able to show that from this violation one can self-test the corresponding quantum state. Remarkably, these inequalities are constituted by an amount of terms that scales linearly with the system

size. Lastly, we show that the introduced method has the potential to be generalised to other families of multipartite states.

1.2.4 Verification of quantum optimizers

The main motivation behind the construction of larger and better quantum computers is to demonstrate the so-called quantum advantage, that is, to show that there is a problem that those devices can solve in a more efficient way than any classical computer can. Recently, a lot of interest has been attracted by quantum optimizers, namely quantum computers that are specialised in solving specific optimisation problems for which no efficient classical algorithm is known.

A prototypical example of hard optimisation problem is that of finding the ground states of classical Ising models, that is, hamiltonians of systems of classical spins. Such energy minimisation problem is particularly interesting because it finds applications in a huge variety of fields: indeed, ground states of Ising models are capable of encoding the solution to important decision and optimisation problems that come from risk assessment in finance or machine learning, among others [Luc14].

Given both the relevance and the hardness of the question, it comes with no surprise that a plethora of approximate but more scalable classical energy minimisation algorithms have been introduced. Hence, a natural comparison that has been extensively studied is that between the solution provided by newly developed quantum optimizers and these efficient classical algorithms. Nevertheless, all these optimisation methods - both quantum and classical - share a crucial drawback, namely the fact that they provide only upper bounds to the ground state energy of interest.

Hence, apart from showing that quantum optimizers find better upper bounds than classical energy minimisation techniques, a very timely question to address is how to certify that their output is actually close to the exact minimum. To answer that, a very informative tool is constituted by methods that provide lower bounds to the ground state energy.

Contribution: We study a hierarchy of relaxations of the classical Ising ground state energy problem in the form of semidefinite programs. A relevant property of these relaxations is that they can provide both lower and upper bounds to the exact solution with a polynomial effort in the size of the system. We also augment the method by leveraging two additional tools. First, we improve its scalability by means of the so-called chordal extension, a technique that can exploit the sparsity of the problem in a systematic way. Second, we adopt a strategy referred to as branch-and-bound that allows to combine lower and upper bounds so to

converge to the exact ground state energy. We benchmark the introduced method with the D-Wave 2000Q quantum annealer and find instances where the latter is unable to reach the ground-state configuration, hence being stuck in a local minimum.

Chapter 2

Preliminaries

2.1 Convex optimisation in quantum information theory

Finding the global minimum of a function $f(x)$ over a set of variables $x \in \mathbb{R}^n$ is a problem that has countless applications in all fields of both fundamental and applied science. Despite its great interest stimulates a lot of research in the topic, no general method providing a solution to any minimisation problem in an efficient way is yet known. Interestingly, this picture changes if one restricts the problem to the subcase of convex optimisation, that comprises the cases where both the function and the set over which the optimisation is performed are convex[1]. Indeed, extensive research showed that there exist algorithms to solve these problems efficiently, that is, with a provably polynomial amount of resources [BV04].

Remarkably, a broad variety of optimisation problems can actually be cast in the form of convex ones and those appearing in quantum information theory are no exception to this phenomenon. In fact, in many of the scenarios considered in the context of quantum information protocols, one is precisely interested in characterising properties of convex sets. That is the case, among others, of the set of quantum states, separable states, completely positive quantum channels, as well as the sets of local, quantum and no-signalling correlations in the device-independent framework. Therefore, it comes with no surprise that convex optimisation tools play a central role in quantum information theory, with a particular attention to the special cases of linear and semidefinite programming. Moreover,

[1]Recall that a function $f(x)$ is convex if it satisfies the inequality $f(\alpha x_1 + \beta x_2) \leq \alpha f(x_1) + \beta f(x_2)$ for any positive coefficients α and β that sum up to one. Similarly, a set $S \subset \mathbb{R}^n$ is convex if for any two points $x_1, x_2 \in S$, their convex combination $\alpha x_1 + \beta x_2$ belongs to S as well.

even in the cases in which either the function or the considered set (or both of them) are not convex, it is often possible to consider *relaxations* expressed in terms of a convex optimisation problem, which allow for an efficient computation of lower bounds to the minimum of interest.

Here we focus on two specific examples of convex optimisation problems: the cases of linear and semidefinite programming. Later, we revise the case of a convex relaxation to the generally non-convex problem of constrained polynomial optimisation.

2.1.1 Linear programming and polytopes

Linear programming (LP) is the problem of minimising a linear function subject to linear equality and inequality constraints. In its standard or *primal* form, a general linear programming problem is usually written as

$$\begin{aligned} \text{minimise } & c^T x \\ \text{s.t. } & Ax = b\,, \\ & x \geq 0\,, \end{aligned} \tag{2.1}$$

where $A \in \mathbb{R}^{m\times n}$, $b \in \mathbb{R}^m$, $x \in \mathbb{R}^n$ and the inequality $x \geq 0$ is interpreted componentwise, that is $x_i \geq 0$ for $i = 1, \ldots, n$. Geometrically, LP problems have a nice interpretation in terms of their feasible set, i.e. the set over which the optimisation is performed. Indeed, the feasible set of (2.1) is the intersection of an affine subspace (defined by the constraints $Ax = b$) and the non-negative orthant (represented by the points satisfying $x \geq 0$) and, being an intersection of two convex sets, it is clearly convex.

In general, a set defined by a finite collection of linear inequalities and equalities is called polyhedron. For the purposes of this thesis, we are only interested in cases where the feasible set is bounded, thus constituting what is called a *polytope*. The geometry of polytopes is very well understood: in particular, the Minkowski-Weyl theorem [Zie12] states that any polytope P can be expressed as the convex hull of a finite amount of extremal points, namely

$$P = \text{ conv } (v_1, \ldots, v_s) = \left\{ \sum_{i=1}^{s} \lambda_i v_i \,\middle|\, \sum_{i=1}^{s} \lambda_i = 1\,,\ \lambda_i \geq 0\,,\ i = 1, \ldots, s \right\}. \tag{2.2}$$

The set of vectors $v_i \in \mathbb{R}^n$ is usually referred to as *vertices* of the polytope. As already pointed out, polytopes can equivalently be defined by a finite set of inequalities. The minimal amount of inequalities required to define P is called its *facets*. Given the facet representation of a polytope,

determining the list of its vertices is usually called *vertex enumeration* problem. Conversely, deriving the complete set of facets corresponding to a vertex representation is known as solving the *convex hull* problem. Algorithms for solving both tasks are known and have been implemented in software [Fuk97, Avi00]. Notice that the best algorithm for finding the list of facets (vertices) for a polytope composed of n vertices (facets) in a space of dimension d has a worst-case time complexity that scales as $O(n^{\lfloor d/2 \rfloor})$ [Cha93].

Importantly, to any primal form of a LP problem is associated the following *dual* problem

$$\begin{aligned} &\text{maximise } b^T y \\ &\text{s.t. } A^T y \leq c\,. \end{aligned} \tag{2.3}$$

Notice that (2.3) defines a maximisation over a polyhedral set as well. Moreover, there is a strong algebraic relation between any feasible solution x^* of a primal LP problem and any solution y^* of its dual. The relation is called *weak duality* and it states that $c^T x^* \geq b^T y^*$. In practice, it means that any feasible dual solution can be used to lower bound the value of the primal and, conversely, any feasible primal solution provides an upper bound for the dual problem. Remarkably, it is known that whenever both the primal and the dual problem are feasible, then the equality holds, corresponding to the case of *strong duality*.

In practice, linear programming problems are interesting because they can be solved efficiently. More precisely, many algorithms are known that provide solutions in polynomial time and are currently implemented in software, such as interior points methods [Kar84, RTV97].

2.1.2 Projecting and intersecting polytopes

Before moving to the more general case of semidefinite programming, let us discuss how to characterise polytopes restricted to subspaces. More precisely, we consider a scenario where the complete description (either through vertices or through facets) of a polytope is known, but one is interested in its representation in a given subspace. There are two relevant operations to explore, namely projection and intersection.

Let us start with analysing the first: consider a subspace $V \subset \mathbb{R}^d$ and denote by $\pi_V : \mathbb{R}^d \to V$ the projection onto it. Imagine then that we want to project a given polytope $P \subset \mathbb{R}^d$ onto V. There are two ways of determining the action of π_V on P. First, $\pi_V(P)$ can be straightforwardly

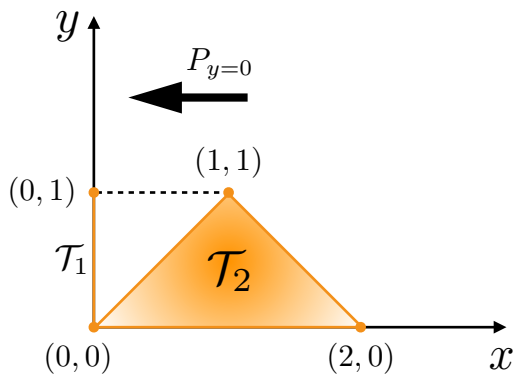

Figure 2.1: Example of projection of a triangle onto the y axis. The vertices of the triangle are the set $\{(0,0),(2,0),(1,1)\}$, whose projection are the points $\{(0,0),(0,1)\}$. Therefore the desired projected polytope is the set $0 \leq y \leq 1$. Conversely, the intersection of the triangle with the y axis coincides with the point $(0,0)$.

defined in terms of projection of its vertices, i.e.,

$$\pi_V(P) = \left\{ p \in V \,|\, p = \sum_{i=1}^{s} \lambda_i \pi_V(v_i) \;,\; \lambda_i \geq 0 \;,\; \sum_{i}^{s} \lambda_i = 1 \right\}. \qquad (2.4)$$

Notice that the projections of the vertices v_i, $\pi_V(v_i)$ might not be vertices of the projected polytope $\pi_V(P)$. On the other hand, a vertex of $\pi_V(P)$ must come from a vertex of P under the projection π_V.

However, in certain situations it is much easier to describe a polytope by using inequalities instead of vertices. In such a case it is thus impossible to use (2.4) in order to find $\pi_V(P)$, and one needs to exploit the facets of P for that purpose. A method that does the job is the so-called Fourier-Motzkin elimination [Sch98], which allows one to find facets of $\pi_V(P)$ starting from facets of P.

Let us now briefly describe this method starting from an illustrative bidimensional example: suppose that we want to project the triangle shown in Figure 2.1 onto the y axis. It is easy to see that the inequalities defining such geometrical object are

$$x + y \leq 2, \quad -x + y \leq 0, \quad y \geq 0. \qquad (2.5)$$

If we cancel out the x coordinate from the inequalities, as we would have done when projecting vertices, we obtain the following three inequalities: $y \leq 2$, $y \leq 0$ and $y \geq 0$, which is not the projection we want since it

defines only a single point $y = 0$. For further purposes, we notice that the result of this procedure coincides with the intersection of the polytope with the $x = 0$ axis, instead of the projection. Thus, projecting facets is a different task than projecting vertices: while for the latter it is enough to map each original vertex into the projected one, the above example shows that this procedure does not work for inequalities.

The basic principle of the Fourier-Motzkin elimination procedure is the fact that any convex combination of two facets of a polytope defines another valid inequality for it. To be more precise, let us consider a polytope $P \subset \mathbb{R}^d$ for some finite d, and let $f_1 \cdot p \leq \beta_1$ and $f_2 \cdot p \leq \beta_2$ be inequalities defining two different facets of it; here, $f_1, f_2 \in \mathbb{R}^d$ and $\beta_1, \beta_2 \in \mathbb{R}$, and $p \in P$. It is clear that any vector p satisfying both these inequalities obeys also the following inequality

$$[\lambda f_1 + (1-\lambda)\, f_2] \cdot p \leq \lambda\beta_1 + (1-\lambda)\,\beta_2 \tag{2.6}$$

for any $0 \leq \lambda \leq 1$. The Fourier-Motzkin elimination exploits this property in order to define new valid inequalities bounding the polytope in which the coordinate that we want to project out is no longer involved. Coming back to the triangle example, we notice that by taking a convex combination with $\lambda = 1/2$ of the first two inequalities in (2.5) we get a new inequality that involves only y, i.e., $y \leq 1$. If we consider in addition the third inequality, that does not contain x, we get the right projection of the triangle, that is the set $0 \leq y \leq 1$, as shown in Figure 2.1.

Let us now state the general procedure of the Fourier-Motzkin elimination. Given a generic polytope in $\mathbb{R}^d$ defined by a finite set of inequalities $f_i \cdot p \leq \beta_i$, where $f_i \in \mathbb{R}^d$ and $\beta_i \in \mathbb{R}$, the list of inequalities defining its projection in the subspace defined by $p_i = 0$ for some i, is obtained through the following steps:

- divide the list of inequalities according to the sign of the coefficient in front of p_i to obtain three sub-lists f_{i_+}, f_{i_-},f_{i_0} corresponding to positive, negative or zero coefficient,
- take all the possible convex combinations between one element of f_{i_+} and one of f_{i_-}, choosing the proper combination in order to get a new valid inequality with zero coefficient in front of p_i,
- the obtained list, together with f_{i_0}, gives a complete set of inequalities that defines the projected polytope,
- remove all the redundant inequalities to get the minimal set.

The main problem with the Fourier-Motzking elimination method is that it is in general very costly in terms of computational requirements.

Indeed, due to the redundancy that one gets at each step, the time and memory needed to eliminate the variables scale exponentially with the number of variables that one wants to project out.

Another operation that we exploit in this thesis is an intersection of a polytope P with a given subspace. To define it let us consider again a linear space $\mathbb{R}^d$ and its subspace $V \subset \mathbb{R}^d$. Then, the intersection operation, denoted $\text{int}_V : \mathbb{R}^d \longrightarrow V$ is defined as

$$\text{int}_V(P) = \{p \in P \,|\, p \cdot w = 0 \;\text{ for all }\; w \in V^\perp\}, \tag{2.7}$$

where $V^\perp$ is the subspace of $\mathbb{R}^d$ orthogonal to V. It is not difficult to notice that any element belonging to the intersection of P with V is also an element of its projection onto the subspace, that is

$$\text{int}_V(P) \subseteq \pi_V(P). \tag{2.8}$$

Moreover, contrarily to the projection, the intersection of a polytope is more easily described in the dual representation. To show how, we define the dual basis $\{\vec{v}_i^*\}$ and $\{\vec{w}_j^*\}$ for the dual of the subspaces V and $V^\perp$, respectively, so to decompose any inequality in P^* as $\vec{f} = \sum_i f_i \vec{v}_i^* + \sum_j f_j \vec{w}_j^*$. Then, we can define

$$\text{int}_V(P)^* = \left\{ g \in V^* \,|\, g = \sum_i f_i \vec{v}_i^* \;\text{ where }\; f_i = \vec{f} \cdot \vec{v}_i^* \;\text{ for }\; \vec{f} \in P^* \right\}. \tag{2.9}$$

Lastly, we also notice that (2.8) implies, for the dual representation

$$\text{int}_V(P)^* \supseteq \pi_V(P)^*, \tag{2.10}$$

meaning that some inequalities valid for the intersection of the polytope might be not valid for its projection. In other words, there are generally inequalities in $\text{int}_V(P)^*$ that cannot be written as a convex combination of the original ones in P^*.

2.1.3 Semidefinite programming

Semidefinite programming is a broad generalisation of linear programming, representing the case of optimisation of a linear function subjected to linear matrix inequalities. Let us denote by $\mathcal{S}^n$ the set of symmetric real $n \times n$ matrices. Recall that a matrix $A \in \mathcal{S}^n$ is said to be positive semidefinite and denoted by $A \succeq 0$ if it satisfies $v^T A v \geq 0$ for any vector $v \in \mathbb{R}^n$. The set $\mathcal{S}^n_+$ of positive semidefinite $n \times n$ matrices is a cone,

hence a convex subset of $\mathcal{S}^n$. Then, a general semidefinite programming (SDP) problem can be stated in its *primal* form as

$$\begin{aligned} \text{minimise} \quad & \langle C, X \rangle \\ \text{s.t.} \quad & \langle A_i, X \rangle = b_i \,, \qquad i = 1, \ldots, m \,, \\ & X \succeq 0 \,, \end{aligned} \tag{2.11}$$

where A_i, C are symmetric $n \times n$ matrices and $\langle X, Y \rangle := \operatorname{tr}(XY)$. Similarly to the linear programming case, the feasible set of an SDP is the intersection of the affine subspace defined by $\langle A_i, X \rangle = b_i$ and the positive semidefinite cone $\mathcal{S}^n_+$, hence it is also convex. More precisely, the set of matrices satisfying the constraints in (2.11) is generally called a spectrahedron and, unlike the feasible set of a LP, it will generally not be a polyhedron. In particular, this implies that spectrahedra cannot be defined by a finite amount of linear inequalities.

As for the formulation of LP problems, the primal form of an SDP can also be associated to its *dual* problem, which reads as follows

$$\begin{aligned} \text{minimise} \quad & b^T y \\ \text{s.t.} \quad & \sum_{i=1}^{m} A_i y_i \preceq C \,, \end{aligned} \tag{2.12}$$

where $b = (b_1, \ldots, b_m)$ and $y = (y_1, \ldots, y_m)$ are the dual decision variables. Remarkably, weak duality between dual and primal problems holds for SDPs as well, allowing one to use the feasible solutions of one to bound the values of the other. The conditions for strong duality are however more stringent than in the linear programming case. In particular, strong duality holds if both problems are strictly feasible, meaning that there exists a $X \succ 0$ that satisfies the constraints in the primal problem (2.11) and, on the dual side, there exist a vector y for which $C - \sum_{i=1}^{m} A_i y_i \succ 0$.

From a practical point of view, SDPs can provably be solved efficiently, that is, with algorithms that provide a solution in polynomial time [VB96]. In terms of software implementation, many packages are known that work as parsers (i.e. softwares that take care of casting a generic SDP into its standard primal or dual form) such as CVX [Cvx] and YALMIP [Yal] and solvers (i.e. software packages implementing numerical algorithms to solve SDPs), such as MOSEK [Mos] and SDPA [Sdpa].

2.1.4 The moment problem and polynomial optimisation

Consider the following problem: take a set of n random variables $x_1, \ldots, x_n$ that can take real values inside some compact set $S = \{x \in \mathbb{R}^n \,|\, g_1(x) \geq$

$0, \ldots, g_m(x) \geq 0\}$, distributed according to some non-negative measure $\mu : \mathbb{R}^n \to \mathbb{R}^+$. Assume that one has access to some of the expectation values or *moments* of such probability measure, namely the numbers

$$\langle x^\alpha \rangle = \int x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} \mu(dx) \ , \tag{2.13}$$

where, for instance, only moments up to some degree d are considered, that is those that satisfy $\sum_i \alpha_i \leq d$. A very relevant question to ask is, given a finite set of such moments, how to check whether they are indeed compatible with a valid probability measure. In other words, which are the constraints that the numbers $\langle x^\alpha \rangle$ have to respect so to allow the construction of a measure μ^* that reproduces them according to (2.13)? This question is usually referred to as the *truncated moment problem* and it cannot be answered with a simple and self-contained test in the general multivariate case (i.e. with $n > 1$). Interestingly enough, it is however possible to introduce an infinite sequence of SDP conditions that approximate the set of valid moments arbitrarily well.

The idea on which these conditions are based can be introduced as follows: take an arbitrary polynomial $q(x) = \sum_\alpha q_\alpha x^\alpha$ of degree at most ν in the variables x. By taking into account that the expectation value of its square is positive for any measure, one derives

$$\langle q(x)^2 \rangle = \sum_{\alpha,\beta} q_\alpha q_\beta \langle x^\alpha x^\beta \rangle = \vec{q}^T \Gamma^{(\nu)}(x) \vec{q} \geq 0 \tag{2.14}$$

where we have introduced the vector $\vec{q}$ with components q_α indexed by $\alpha = \alpha_1, \ldots, \alpha_n$ and the matrix Γ, usually referred to as *moment matrix*, that has entries $\Gamma^{(\nu)}_{\alpha,\beta}(x) = \langle x^\alpha x^\beta \rangle$. The fact that the condition (2.14) has to be satisfied by any vector $\vec{q}$ of any degree ν directly implies that the moment matrix $\Gamma^{(\nu)}(x)$ constructed from a general measure μ has to be positive semidefinite. Recall that we consider measures that have support on a compact set S defined by a finite amount of polynomial inequalities $g_i(x) \geq 0$. We can therefore use also those conditions to obtain

$$\langle g_i(x) q(x)^2 \rangle = \sum_{\alpha,\beta} q_\alpha q_\beta \sum_\gamma g_{i,\gamma} \langle x^\alpha x^\beta x^\gamma \rangle = \vec{q}^T \Gamma^{(\nu)}(g_i x) \vec{q} \geq 0 \tag{2.15}$$

where we have defined m different *localising matrices* $\Gamma^{(\nu)}(g_i x)$ associated to the polynomial constraints $g_i(x) \geq 0$ and whose entries are defined as $\Gamma^{(\nu)}(g_i x)_{\alpha,\beta} = \sum_\gamma g_{i,\gamma} \langle x^\alpha x^\beta x^\gamma \rangle$. It follows from (2.15) that moments associated to any measure supported on S always produce non-negative localising matrices. Notice that $\Gamma^{(\nu)}(x)$ contains moments of order up to 2ν while the localising matrices $\Gamma^{(\nu)}(g_i x)$ involve moments of order

smaller or equal to $2\nu + d_i$, where d_i is the degree of the polynomial $g_i(x)$.

The above considerations allow one to devise a hierarchy of tests to check whether a given collection of numbers $\langle x^\alpha \rangle$ are compatible moments of the same probability measure. The level l of such hierarchy is constructed as follows: take the moment matrix $\Gamma^{(l)}(x)$ and the localising matrices $\Gamma^{(\nu_i(l))}(g_i x)$ of the order chosen to satisfy $\nu_i(l) + \lfloor d_i/2 \rfloor = l$. The entries of these matrices correspond to the numbers $\langle x^\alpha \rangle$ and, depending on the level l, to some unassigned variables associated to higher order moments. The test, at level l, consists in checking whether those numbers are compatible with positive semidefinite moment and localising matrices, which is a question that can be efficiently solved as an SDP. Importantly, for any finite level there are numbers that give rise to non-negative $\Gamma^{(l)}(x)$, $\Gamma^{(\nu_i(l))}(g_i x)$ that cannot be associated to any probability measure. This implies that the corresponding SDP can only provide a necessary condition for moment compatibility. Moreover, increasing the level provides more and more stringent conditions, since the matrices for level l always contain as submatrices those of lower levels $l' \leq l$. Remarkably, this hierarchy of SDP tests defines a convergent series of outer approximation to the set of compatible moments, meaning that any collection of numbers that does not correspond to moments of a probability measures has to fail the test at some finite level [Las01b].

To give a concrete example, let us consider the case of two random variables x_1 and x_2 defined on a circle, delimited by the following inequality $g(x) = 1 - x_1^2 - x_2^2 \geq 0$. The moment matrix at level $l = 2$ reads

$$\Gamma^{(2)}(x) = \begin{pmatrix} 1 & \langle x_1 \rangle & \langle x_2 \rangle & \langle x_1^2 \rangle & \langle x_1 x_2 \rangle & \langle x_2^2 \rangle \\ \langle x_1 \rangle & \langle x_1^2 \rangle & \langle x_1 x_2 \rangle & \langle x_1^3 \rangle & \langle x_1^2 x_2 \rangle & \langle x_1 x_2^2 \rangle \\ \langle x_2 \rangle & \langle x_1 x_2 \rangle & \langle x_2^2 \rangle & \langle x_1^2 x_2 \rangle & \langle x_1 x_2^2 \rangle & \langle x_2^3 \rangle \\ \langle x_1^2 \rangle & \langle x_1^3 \rangle & \langle x_1^2 x_2 \rangle & \langle x_1^4 \rangle & \langle x_1^3 x_2 \rangle & \langle x_1^2 x_2^2 \rangle \\ \langle x_1 x_2 \rangle & \langle x_1^2 x_2 \rangle & \langle x_1 x_2^2 \rangle & \langle x_1^3 x_2 \rangle & \langle x_1^2 x_2^2 \rangle & \langle x_1 x_2^3 \rangle \\ \langle x_2^2 \rangle & \langle x_1 x_2^2 \rangle & \langle x_2^3 \rangle & \langle x_1^2 x_2^2 \rangle & \langle x_1 x_2^3 \rangle & \langle x_2^4 \rangle \end{pmatrix} \tag{2.16}$$

Correspondingly, since the constraint $g(x)$ is of degree 2, the localising matrix for a test at level $l = 2$ is chosen to be at order one, hence

$$\Gamma^{(1)}(gx) = \begin{pmatrix} 1 - \langle x_1^2 \rangle - \langle x_2^2 \rangle & \langle x_1 \rangle - \langle x_1^3 \rangle - \langle x_1 x_2^2 \rangle & \langle x_2 \rangle - \langle x_1^2 x_2 \rangle - \langle x_2^3 \rangle \\ \langle x_1 \rangle - \langle x_1^3 \rangle - \langle x_1 x_2^2 \rangle & \langle x_1^2 \rangle - \langle x_1^4 \rangle - \langle x_1^2 x_2^2 \rangle & \langle x_1 x_2 \rangle - \langle x_1^3 x_2 \rangle - \langle x_1 x_2^3 \rangle \\ \langle x_2 \rangle - \langle x_1^2 x_2 \rangle - \langle x_2^3 \rangle & \langle x_1 x_2 \rangle - \langle x_1^3 x_2 \rangle - \langle x_1 x_2^3 \rangle & \langle x_2^2 \rangle - \langle x_1^2 x_2^2 \rangle - \langle x_2^4 \rangle \end{pmatrix} \tag{2.17}$$

Let us also mention that the SDP approach to the truncated moment problems finds applications in the field of polynomial optimisation. Sup-

pose that one is interested in finding the minimum of a polynomial $q(x) = \sum_\alpha q_\alpha x^\alpha$ of some commuting real variables over a compact set S. As noticed by Lasserre [Las01b], one can replace the above optimisation problem with the following

$$q^* = \min_{\mu \in \mathcal{P}(S)} \int q(x)\mu(dx) \tag{2.18}$$

where $\mathcal{P}(S)$ is the space of probability measures on S. Not only the two minimisation problems are equivalent, but one can then see that (2.18) corresponds to minimising a linear function $\langle q(x) \rangle = \sum_\alpha q_\alpha \langle x^\alpha \rangle$ over the space of moments compatible with a probability measure on S. Hence, one can use the previously introduced series of SDP conditions to define a hierarchy of relaxation of any commuting polynomial optimisation problem. More specifically, at level l the minimisation (2.18) is replaced by the following semidefinite program

$$\begin{aligned} \text{minimise} \quad & \sum_\alpha q_\alpha \langle x^\alpha \rangle \\ \text{s.t.} \quad & \Gamma^{(l)}(x) \succeq 0, \\ & \Gamma^{(l)}(g_i x) \succeq 0, \qquad i = 1, \ldots, m\,. \end{aligned} \tag{2.19}$$

Since the minimisation is carried over a set larger than the allowed one, the optimisation is indeed a relaxation of the original problem and generally leads to lower bounds q_l to the optimum q^* (see Fig. 2.2 for a pictorial representation). Moreover, as the SDP condition gets more and more stringent while increasing the level, one obtains a series $q_1 \leq q_2 \leq \ldots \leq q^*$ converging to the exact minimum in the asymptotic limit. Interestingly, depending on the polynomial - and the minimisation set S - one is considering, the convergence might be achieved even at a finite step in the hierarchy. Notice that neither $q(x)$ is generally a convex function nor the set S has to be convex, thus finding q^* is a very hard optimisation problem. Remarkably, the hierarchy introduced by Lasserre provides relaxations in terms of convex optimisation problems, which can be solved much more efficiently.

To conclude, we stress that the techniques presented in this Section directly apply to minimisation problems over variables that take a discrete set of values. Indeed, such sets can be expressed in terms of polynomial inequality constraints, thus falling into the category of sets S considered above. Let us show how by considering the example of dichotomic variables, that is x_i that take only ± 1 values. Clearly such condition can be enforced by imposing the equality constraints $x_i^2 = 1$, which in turn are equivalent to the pairs of inequalities $x_i^2 \leq 1$ and $x_i^2 \geq 1$.

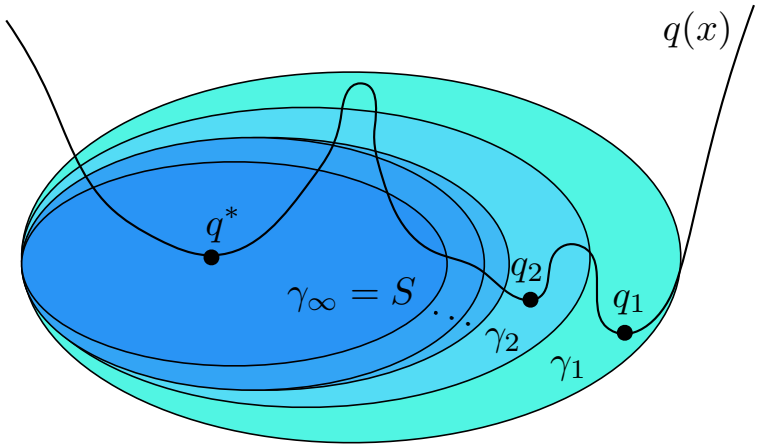

Figure 2.2: Graphical representation of the hierarchy of relaxations to a polynomial optimisation problem. Geometrically, one can represent the sets of moments γ_l compatible with the SDP condition at level l as outer approximations of the set of valid moments on S. Since the optimisation is carried over larger sets than the one of interest, the SDPs generally lead to lower bounds $q_1 \leq q_2 \leq \ldots \leq q^*$ to the minimum of $q(x)$.

2.2 Entanglement

Entanglement is beyond any doubt one of the key properties of quantum mechanics, as first noticed by Schroedinger [Sch35], who also coined the term. Mathematically, it is nothing more than a consequence of the superposition principle applied to composite systems. However, its physical consequences deeply differentiate the behaviour of quantum particles from what could be predicted by classical physics. Entanglement was also the key argument behind a heated debate, initiated by [EPR35], about whether or not quantum theory could be considered complete in its attempt at giving a realistic description of nature.

Beyond its fundamental relevance, which was recognised since the initial formulation of quantum mechanics, entanglement is now identified as a crucial ingredient for most of the paradigmatic protocols in quantum information. The first application that was proposed was in the context of cryptography [Eke91]. After that, a plethora of results have followed and nowadays entanglement plays a key role in many different applications, ranging from quantum communication [BBC$^+$93] to quantum computation [BBD$^+$09] and quantum metrology and sensing [GLM04].

Here we revise the main notions related to bipartite and multipar-

tite entanglement, together with some of the most relevant entanglement detection techniques. Lastly, we present some examples of multipartite states that will be considered in the rest of this thesis.

2.2.1 Characterisation of entanglement

Quantum states are represented by unit trace, positive semidefinite operators acting on a Hilbert space $\mathcal{H}$. Throughout the rest of this thesis, we will work with finite-dimensional complex Hilbert spaces, hence we assume $\mathcal{H} = \mathbb{C}^d$. The set of bounded linear operators acting on such a space is commonly denoted by $\mathcal{B}(\mathcal{H})$. By choosing an orthogonal basis of the space $\{|i\rangle\ ,\ 1 \leq i \leq d\}$, one can identify each element of $\mathcal{B}(\mathcal{H})$ as a $d \times d$ matrix with complex entries. The set of quantum states, also commonly referred to as density matrices, constitutes thus the subspace of $\mathcal{B}(\mathcal{H})$ composed by operators with non-negative eigenvalues and trace one. More formally, we define such space as $\mathcal{D}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \succeq 0\ ,\ \mathrm{tr}\,(\rho) = 1\}$.

To define entanglement one has to consider composite systems. Let us then introduce the concept by starting with the simplest case of two particles. Imagine that two spatially separated parties, Alice and Bob, own one particle each of a bipartite quantum system. The physical degrees of freedom of Alice's particle may then be assigned to a local Hilbert space $\mathcal{H}_A$ of dimension d_A, and similarly, Bob's subsystem is assigned to a space $\mathcal{H}_B$ of dimension d_B. A generic state of the composite system is thus represented by a density matrix acting on the tensor product space $\mathcal{H}_{\mathcal{AB}} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Consider now a composite state that factorises as $\rho = \rho^A \otimes \rho^B$, where ρ^A and ρ^B are some given density matrices acting on the local spaces of Alice and Bob respectively. States of those kind are called *product states* and don't display any kind of correlations: physically, they can be easily obtained by locally preparing the states of Alice‘s and Bob‘s share, without any communication needed between the two parties. More generally, a bipartite state is denoted *separable* if it can be decomposed as a convex combination of product states, that is

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B\ , \quad \sum_i p_i = 1\,, \quad p_i \geq 0\,. \tag{2.20}$$

Separable states represent composite systems than can be correlated by classical means, namely by allowing the parties to act with local operations assisted with classical communication (LOCC) [Wer89]. Physically, this represents the possibility for Alice and Bob to have a source of randomness that outputs an outcome i with probability p_i and then, upon

communicating to each other that a given outcome has occurred, prepare locally the corresponding product state $\rho_i^A \otimes \rho_i^B$. Notice that separable states represent a convex subset of the set of allowed bipartite states $D(\mathcal{H}_{AB})$. Any state that is not separable lies outside such subset and is termed *entangled*. Entangled states are intuitively considered to be correlated in a non-classical way. By its very definition, entanglement is a a resource whose preparation requires more than an LOCC protocol, such as a joint quantum interaction between the subsystems. For this reason, entangled states constitute natural candidates to display quantum features that can provide some advantage in quantum information protocols.

2.2.2 Detection techniques

A very relevant question to ask is how to determine whether a given quantum state is entangled. This is usually referred to as the *separability problem* and despite many attempts, a general solution to it is yet to be found. In fact, the separability problem has been shown to belong to the NP-hard class [Gur03, Gha08]. Here we review some of the most common and useful entanglement detection criteria, starting with the bipartite scenario (for a geometrical representation of entanglement detection, see Figure 2.3).

Let us suppose at first that the state of a composite two-particle quantum system is known. By properly choosing a basis for each local Hilbert space, the corresponding density matrix can then be expanded as

$$\rho = \sum_{i_A,j_A=1}^{d_A} \sum_{i_B,j_B=1}^{d_B} \rho_{i_A j_A, i_B j_B} |i_A\rangle\langle j_A| \otimes |i_B\rangle\langle j_B| \tag{2.21}$$

Detecting the entanglement of ρ corresponds to determining whether it can be written as a convex combination of the form (2.20). A well known technique to rule out such a possibility is the so-called *PPT criterion* [Per96]. It is based on introducing the notion of the partial transposed state with respect to one of the parties: more precisely, starting from the decomposition (2.21), the partial transpose with respect to Alice is defined as the matrix

$$\rho^{T_A} = \sum_{i_A,j_A=1}^{d_A} \sum_{i_B,j_B=1}^{d_B} \rho_{i_A j_A, i_B j_B} |j_A\rangle\langle i_A| \otimes |i_B\rangle\langle j_B| \tag{2.22}$$

and similarly one can define ρ^{T_B} by swapping the density matrix elements on Bob's side. One can show that any separable state has positive partial

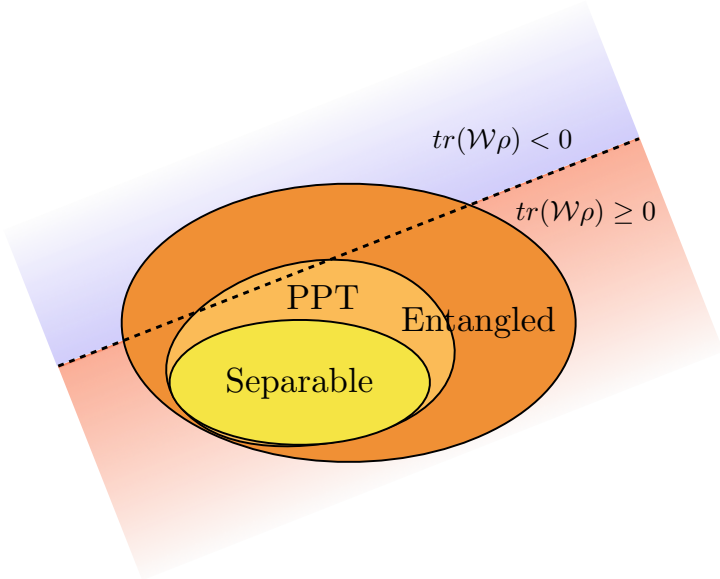

Figure 2.3: Schematic bidimensional representation of the convex sets of separable states, states with positive partial transpose (PPT states) and of all quantum states. States falling outside the separable set are entangled (represented in the orange regions). While every separable state has a positive partial transpose, there are entangled PPT states (light orange region), indicating that the PPT entanglement criterion defines only an outer approximation to the separable set. Nevertheless, any entangled state can be detected by means of an entanglement witness, which geometrically represents a hyperplane separating the separable set from the other states.

transpose (i.e. it is PPT) with respect to both parties, that is, both ρ^{T_A} and ρ^{T_B} are positive semidefinite operators. Checking for a positive partial transpose therefore serves as an entanglement detection technique, since it is a necessary condition for separability. However, except for few cases (namely the cases $d_A = d_B = 2$ and $d_A = 2, d_B = 3$), it is not a sufficient condition, that is, there exist states whose entanglement can not be detected by the PPT criterion [HHH01].

Many generalisations of the PPT criterion have been introduced over the years, based on replacing the transpose map with other positive but not completely positive maps [Bre06, CK07, Pia06, HH99]. Also other separability criteria have been considered [CW03], but all of the approaches known so far fail at detecting some entangled states .

A powerful algorithmic approach is the one of the *symmetric extension*

method [DPS02]. It is based on the idea that one can associate to any separable state (2.20) the so-called symmetric extension

$$\rho^{(ABB_1)} = \rho = \sum_i p_i \rho_i^A \otimes \rho_i^B \otimes \rho_i^{B_1}\,, \quad \sum_i p_i = 1\,, \quad p_i \geq 0\,, \tag{2.23}$$

with the following properties: a) it is PPT with respect to any partition, b) its reduced state with respect to both B and B_1 equals to ρ itself and c) it is symmetric under exchange of B and B_1. Given a known bipartite state, asking whether it is compatible with such a symmetric extension can be cast into an SDP, providing an efficient numerical method to test for separability. Furthermore, the notion of symmetric extension can be extended to any number of copies $ABB_1 \ldots B_k$ of one party. By proceeding in increasing order of k, one gets a hierarchy of more and more stringent conditions for separability. Interestingly, it was shown [DPS04] that such a hierarchy is capable of detecting any entangled state in the asymptotic limit. In other words, this implies that a state is separable if and only if its infinite symmetric extension $\rho^{(ABB_1 \ldots B_\infty)}$ exists.

Notice that all the above methods have one thing in common: they start from the assumption that the state ρ is known. An interesting entanglement criterion that consists in measuring directly observable quantities was firstly introduced in [HHH96]. It is based on measuring the so-called *entanglement witnesses*, namely operators $\mathcal{W}$ that fulfil the following properties

$$\begin{aligned} &\mathrm{tr}\,(\mathcal{W}\rho) \geq 0 \quad \text{for all separable } \rho_s, \\ &\mathrm{tr}\,(\mathcal{W}\rho) < 0 \quad \text{for at least one entangled } \rho_e \end{aligned} \tag{2.24}$$

Therefore, upon obtaining a negative expectation value for $\mathcal{W}$, one can immediately conclude that the observed state is entangled. Geometrically, entanglement witnesses represent hyperplanes in the space of quantum states, dividing the separable subspace from the rest. Interestingly, because of the convexity of such space, one can prove that for any entangled state there is at least one entanglement witness detecting it [HHH96]. This is nothing more than a consequence of the *separating hyperplane theorem* that is widely used in convex optimisation [BV04].

The fact that entanglement witnesses can be directly measured makes them very appealing for experimental implementations. As we will see in more detail in the next section, this is particularly true for the case of multipartite entangled states.

2.2.3 Multipartite notions of entanglement

So far we have restricted our considerations to the case of two-particle systems but many of the previous concepts straightforwardly extend to the multipartite scenario. Consider an N-particle system shared by parties $A_1, A_2, \dots A_N$: a general quantum state is now represented by a density matrix acting on the tensor product space $\mathcal{H} = \mathcal{H}_{A_1} \otimes \dots \otimes \mathcal{H}_{A_N}$ of single-particle Hilbert spaces with local dimensions d_{A_i}. If one allows only for LOCC operation between the parties, the most general state that can be produced looks as follows

$$\rho = \sum_i p_i \rho_i^{A_1} \otimes \rho_i^{A_2} \otimes \dots \otimes \rho_i^{A_N} \,, \quad \sum_i p_i = 1 \,, \quad p_i \geq 0 \,. \tag{2.25}$$

It is clear that such definition generalises the bipartite decomposition (2.20) and hence the notion of separable state to the multipartite case. However, the multipartite scenario exhibits a much richer entanglement structure, which is captured by different levels of separability conditions. There are many different notions of multipartite separability that can be considered. For further purposes, here we focus on the concept of *k-separability*, firstly introduced in [SU01], which aims at answering the quantitative question: "How many particles in the state are genuinely entangled?".

Physically, the idea is to extend the concept of LOCC operation to cases in which some of the parties are allowed to group and produce entangled states among themselves. More formally, let us define an L_k-partition as a partition of the set of parties $I = \{1, \dots N\}$ into L pairwise disjoint non-empty subsets $\mathcal{A}_l$, such that by joining them one recovers I and the size of each $\mathcal{A}_l$ is at most k parties. We say that a state is separable according to such partition, or L_k-separable, if it can be decomposed in the following way

$$\rho_{L_k} = \sum_i p_i \rho_i^{\mathcal{A}_i} \otimes \dots \rho_i^{\mathcal{A}_L} \,, \quad \sum_i p_i = 1 \,, \quad p_i \geq 0 \,, \tag{2.26}$$

where the $\rho_i^{\mathcal{A}_l}$ denote arbitrary (possibly entangled) states among particles in the subset $\mathcal{A}_l$. Notice that for $k = 1$ we recover the case of (2.25), which is often referred to as a *fully separable* state. It is then clear that a state admitting a decomposition (2.26) for a given L_k-partition can exhibit entanglement among at most k particles, which is the size of the largest allowed subset. The concept of *k-separable* state follows by allowing mixture between different L_k-partitions, so to obtain

$$\rho = \sum_{S \in \mathcal{S}_k} q_s \rho_S, \quad \sum_{S \in \mathcal{S}_k} q_S = 1 \,, \quad q_S \geq 0 \,, \tag{2.27}$$

where $\mathcal{S}_k$ is the set of all possible L_k-partitions of N parties and ρ_S is a separable state of the form (2.26) according to the given partition. Multipartite states that do not admit a decomposition (2.27) for some value k necessarily contain at least $k+1$ entangled particles. Equivalently, they are commonly said to display an amount of *entanglement depth* of $k+1$. Dividing states into different values of entanglement depth defines a hierarchy of more and more entangled multipartite states, ranging from full separability to having entanglement depth equal to N, which is usually called *genuine multipartite entanglement* (GME).

Given its richer structure, detecting multipartite entanglement constitutes both a more interesting and a more challenging question than in the bipartite case. As a first attempt to rule out full separability, one can for instance use the fact that a state of the form (2.25) is separable across any bipartition. Hence, violating any bipartite criterion according to some given partition can be used to detect multipartite entanglement. The symmetric extension hierarchy has also been extended to the multipartite scenario [DPS05] and it has shown to be convergent to the fully separable set of states. Moreover, criteria have been derived to detect genuine multipartite entanglement as well [GS10]. However, the fact that all these methods require the knowledge of the whole state becomes even more problematic as the number of particles grows. Indeed, already for the simplest case of an N-qubit state, a general density matrix ρ is described by a $2^N \times 2^N$ matrix, thus requiring an exponentially increasing amount of information to be handled.

Entanglement witnesses are therefore a very practical solution for entanglement detection, especially when many particles are involved. Even more importantly, any entanglement witness can be estimated by measuring local observables only [GHB$^+$02, Ter02], which makes their experimental implementation particularly convenient. In fact, plenty of entanglement witnesses are known that are suited to detect entanglement for many families of multipartite states [GT09].

Moreover, since the sets of k-separable states are also convex (cfr. their definition (2.27)), from the separating hyperplane theorem we conclude that there exist witnesses suitable to detect multipartite entanglement states that lie outside any of these sets. Indeed, general techniques have been developed to derive witnesses testing against full separability up to the strongest ones apt for GME detection [TG05a, JMG11, TG05b]. Other results have also adapted to the limits of realistic experimental implementations, by deriving witnesses from the ground state energy of local hamiltonians [TG06, TG05b] or nonlinear inequalities detecting entanglement from collective spin measurements [TKGB09].

2.2.4 Important classes of multipartite entangled states

Here we introduce some of the most important families of bipartite and multipartite entangled states, both for their theoretical and experimental relevance. For further purposes we focus on the qubit case, that is, when all the local dimensions are equal to two, $d_{A_i} = 2$ for $i = 1, \ldots, N$. Notice however that all the states presented here can be generalised to higher local dimensions as well.

Let us start with the prototypical maximally entangled bipartite state:

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}} \left[|00\rangle + |11\rangle\right] , \tag{2.28}$$

usually referred to as *Bell state*. Interestingly, one can define a whole basis for the two-qubit Hilbert space constituted by states that are local unitary equivalent to the Bell state, i.e. states obtained by acting on $|\phi^+\rangle$ with tensor products of unitaries $U_1 \otimes U_2$. The resulting Bell basis reads as follows

$$\begin{aligned} \left|\psi^\pm\right\rangle &= \frac{1}{\sqrt{2}} \left[|01\rangle \pm |10\rangle\right] , \\ \left|\phi^\pm\right\rangle &= \frac{1}{\sqrt{2}} \left[|00\rangle \pm |11\rangle\right] . \end{aligned} \tag{2.29}$$

The Bell state is the building block of most of the initial quantum information protocols, starting with quantum cryptography [Eke91], teleportation [BBC$^+$93] and dense coding [BW92].

Historically, the first classes of multipartite states that have been studied can be considered as generalisations of some version of the Bell state to its many-particle counterpart. A first example is the Greenberger-Horne-Zeilinger (GHZ) state [GHZ89]

$$|GHZ_N\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right] , \tag{2.30}$$

which can be seen as the multipartite equivalent of the $|\phi^+\rangle$ state. GHZ states have been extensively studied and find application in several protocols, some examples being quantum metrology [GLM04] and quantum secret sharing [HBcvB99]. They have also been generated in experiments by using many different platforms, ranging from photonic [WLH$^+$18a] to trapped ions [MSB$^+$11] and superconducting circuits [SXL$^+$17] implementations of up to 18, 12 and 10 qubits respectively.

On the other hand, the W state

$$|W_N\rangle = \frac{1}{\sqrt{N}} \left[|0\ldots01\rangle + |0\ldots10\rangle + \ldots + |1\ldots00\rangle\right] , \tag{2.31}$$

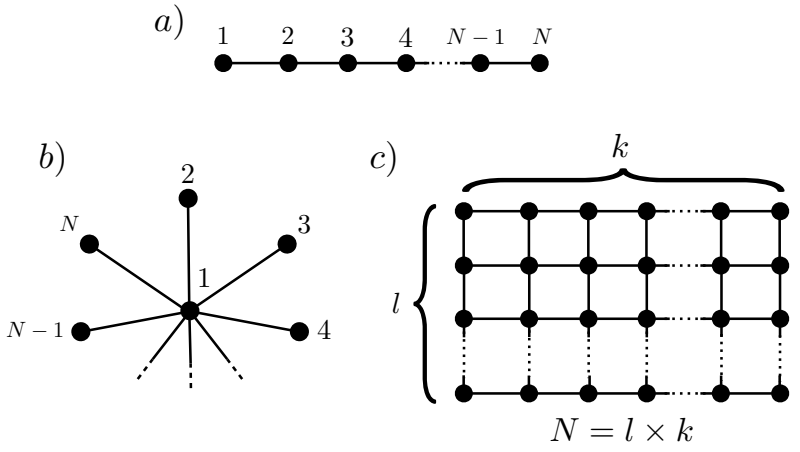

Figure 2.4: Some examples of graphs associated to the most studied graph states: a) The linear cluster state, b) the star graph state, equivalent to the GHZ state, c) the 2D cluster state.

can be seen as a generalisation of the $|\psi^+\rangle$ state, and it is usually described as the state of one excitation symmetrically distributed over all the particles. W states are part of a larger family of multipartite states, the Dicke states [Dic54], which are the symmetric states of k excitations over N particles. Dicke states are experimentally interesting because their entanglement is provably robust under decoherence effects [GBB08]. W states have been generated both with photons [KST$^+$07] and trapped ions [HHR$^+$05].

Lastly, let us introduce the family of *graph states* [HEB04]: consider a graph $G = (V, E)$, where V is the set of vertices of size $|V| = N$, and E is the set of edges connecting the vertices. Let then $n(i)$ be the neighbourhood of the vertex i, i.e., all vertices from V that are connected to i by an edge. Now, to every vertex i we associate an operator

$$G_i = X_i \otimes \bigotimes_{j \in n(i)} Z_j, \tag{2.32}$$

in which the X operator acts on site i, while the Z operators act on all sites that belong to $n(i)$ and X and Z represent two of the Pauli matrices

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{2.33}$$

To each graph G we can associate a graph state $|\psi_G\rangle$ as the unique eigenstate of all these operators G_i $(i = 1, \ldots, N)$ with eigenvalue one. The

G_i's are called stabilizing operators of $|\psi_G\rangle$ and they generate the 2^N-element commutative group of operators stabilizing $|\psi_G\rangle$, called *stabilizer group*. An example of graph state is precisely the GHZ state. Indeed, one can check that the state (2.30) is stabilized by the N commuting operators $G_1 = X_1 \dots X_N$ and $G_i = Z_1 Z_i$ for $i = 2, \dots N$, which are locally unitary equivalent to the stabilizers associated to the star graph (see Figure 2.4.a). Another relevant exponent of the graph-state family is the so-called *cluster state*, which is associated to the 2D lattice graph, shown in Figure 2.4.c, and is the building blocks for measurement based quantum computation [RB01]. Remarkably, graph states appear as codewords in some error correction codes as well [Got96].

Graph states are also interesting because they can be produced by bipartite interactions: indeed, it can be shown that $|\psi_G\rangle$ is obtained by applying to a product state $[(|0\rangle + |1\rangle)/\sqrt{2}]^{\otimes N}$ control-Z gates $CZ_{ij} = (\mathbb{1}_i + Z_i)(\mathbb{1}_j + Z_j)$ between each pair i, j of connected qubits in G. Because of their practical interest, graph states have been experimentally produced both using photons [LZG$^+$07] and ions [LZJ$^+$14].

2.3 Bell nonlocality

Nonlocality is a concept that was first introduced by Bell in 1964 [Bel64] to close a debate regarding the completeness of quantum mechanics, dating back to the Einstein-Podolski-Rosen (EPR) paradox presented in [EPR35]. The authors of such a paradox argued that the postulates of quantum theory had to be emergent properties of a more refined theory involving some degrees of freedom that we are not in control of. Almost thirty years after, Bell made a quantitative statement showing that quantum mechanics is capable of producing correlations that are not reproducible by any such *hidden variable theory* satisfying the two reasonable principles of reality (any property of the system is determined prior to its observation) and locality (particles do not communicate faster than at the speed of light). The non-classicality of these *nonlocal* correlations has been widely studied over the last decades [BCP$^+$14] and, although being introduced as a concept of fundamental interest, it is now a crucial ingredient in many quantum information applications in the so-called device-independent scenario. Moreover, the existence of nonlocal correlations has been confirmed experimentally both in bipartite [FC72, ADR82] and multipartite scenarios [PBD$^+$00, ZHW$^+$15, LZJ$^+$14]. More recently, a series of experiments have achieved the first loophole-free Bell tests, thus confirming Bell's theorem without additional assumptions usually employed to overcome

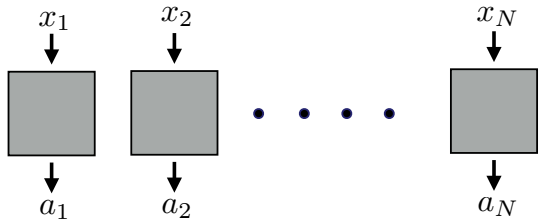

Figure 2.5: Pictorial representation of the device-independent scenario in a multipartite setting. Each of the N observers holds a black box (supposedly containing a particle of a shared physical system) and interacts with it by selecting an input x_i, corresponding to the local measurement choice, and by collecting an output a_i.

experimental imperfections [HBD$^+$15, GVW$^+$15, SMSC$^+$15].

Here we introduce the main concepts of the device-independent picture in the multipartite scenario, focusing on nonlocality as an entanglement detection method. After describing the geometrical characterisation of local, quantum and post-quantum correlations, we explore the various degrees of multipartite nonlocality. Lastly, we present a device-independent certification technique known as self-testing and apply it to a specific example.

2.3.1 The device-independent framework

The most general Bell scenario involves N spatially separated observers $A_1, \ldots, A_N$ sharing a N-partite quantum state ρ. Each A_i is allowed to perform on its local share of the system m possible d-outcome measurements. We denote the measurements for party i as $M_{x_i}^{a_i}$, where $x_i \in \{0, \ldots, m-1\}$ denotes the measurement choice and $a_i \in \{0, \ldots, d-1\}$ represents the possible output. Such a scenario is thus usually described by the three (N, m, d) numbers, specifying number of parties, inputs and outcomes.

By repeating their measurements sufficiently many times, the experimenters can estimate the following conditional probabilities

$$p(a_1, \ldots, a_N | x_1, \ldots, x_N) = \mathrm{tr}\left(M_{x_1}^{a_1} \otimes \ldots \otimes M_{x_N}^{a_N} \rho\right), \tag{2.34}$$

where the $M_{x_i}^{a_i}$ are generic positive-operator valued measures (POVMs), that is, positive semidefinite operators that satisfy $\sum_{a_i} M_{x_i}^{a_i} = \mathbb{1}$. In the modern approach to Bell nonlocality the above scenario is often interpreted in an operational way: the observers are considered to hold each a black-box (supposedly) containing a particle of the quantum system

and to interact with it at each round by providing some classical input x_i and by collecting the corresponding classical output a_i. Importantly, the parties are not allowed to communicate with each other after having chosen the input and before having collected their output (see Figure 2.5). The observers then might be interested in inferring properties of the underlying quantum system by simply looking at the correlations (2.34) observed upon applying local measurements on the state. Similarly, the parties could consider using the collected data to extract a secure cryptographic key or exploiting one (or more) of the outcomes a_i as a source of random bits. All of the above applications, among many others, have been extensively studied and the presented picture is usually termed *device-independent framework*, since all the non-classical properties of the system are inferred or exploited solely at the level of the observed probabilities, without making any assumption on the physical systems contained in the boxes.

According to Bell's definition, introduced in [Bel64], the observed correlations are referred to as *local* if they can be reproduced by the following local hidden variable (LHV) model

$$p(a_1,\ldots,a_N|x_1,\ldots,x_N)=\sum_{\lambda} p_\lambda \prod_{i=1}^{N} p(a_i|x_i,\lambda)\,. \tag{2.35}$$

Similarly to the LOCC paradigm for states, presented in Section 2.2, an LHV model represents the most general form of correlations that can be produced by classical means. Physically, any local distribution can be obtained by having a source of random numbers λ shared by the observers, who then choose their outputs according to the local response function $p(a_i|x_i,\lambda)$, that depends solely on their input and the random variable.

Interestingly, there is a very close connection between separable states and local correlations. To see that, let us suppose that the state in the boxes is separable: then, by (2.25) it follows that the conditional probabilities can be decomposed as

$$p(a_1,\ldots,a_N|x_1,\ldots,x_N)=\sum_{\lambda} p_\lambda \operatorname{tr}\Big(\bigotimes_i M_{x_i}^{a_i}\bigotimes_i \rho_\lambda^{A_i}\Big)\,. \tag{2.36}$$

Notice that the above equation coincides with that of a local model (2.35), if we set each response functions to be $p(a_i|x_i,\lambda)=\operatorname{tr}(M_{x_i}^{a_i}\rho_\lambda^{A_i})$.

Remarkably, there are quantum states that, upon choosing properly some local measurements, are able to produce *nonlocal* correlations, that is, correlations that cannot be described by any LHV model. This was first shown by Bell [Bel64] and it's the content of his famous theorem. By

the previous reasoning, it also follows that states producing nonlocal correlations are necessarily entangled. In other words, observing nonlocality serves as a device-independent way of witnessing entanglement. Apart from entanglement detection, nonlocality has also been shown to be a resource for various device-independent cryptographic protocols, starting with the first security proofs for randomness generation [PAM+10] and key distribution [ABG+07], and for other more sophisticated forms of device-independent certification, such as dimension witnessing [BPA+08] and self-testing [MY04].

2.3.2 Geometrical approach

Finding ways of characterising the correlations that can be achieved by LHV models and quantum theory has implications both from the practical and fundamental point of view. On the one hand, having a good understanding of local correlations provides general tools to detect nonlocality. On the other hand, characterising the set of quantum correlations gives an idea of which limitations are imposed by quantum theory itself on the realisation of quantum information protocols. To mathematically characterise correlations in a Bell scenario, it is useful to adopt a geometrical picture. To do so, let us arrange the probability distributions (2.34) in a vector with $(md)^n$ components, each corresponding to a different choice of inputs $a_1, \ldots, a_N$ and outputs $x_1, \ldots, x_N$. We name any such vector $\vec{P}$.

The Local set

Let us start by studying local correlations in this framework: all vectors $\vec{P}$ obtained by varying over all possible LHV models (2.35) define a geometrical set, the so-called *local set*, which we denote by $\mathcal{L}$. By looking at the definition of LHV model, it is easy to see that such a set is convex. Moreover, it can be shown that $\mathcal{L}$ is actually a polytope. To do so, it is enough to notice that any vector $\vec{P} \in \mathcal{L}$ can be obtained as a convex combination of deterministic strategies, that is, the combination in (2.35) can be replaced by

$$p(a_1, \ldots, a_N|x_1, \ldots, x_N) = \sum_\lambda p_\lambda \prod_i D(a_i|x_i, \lambda)\,, \quad p_\lambda \geq 0\,, \quad \sum_\lambda p_\lambda = 1\,, \tag{2.37}$$

where $D(a_i|x_i, \lambda)$ are deterministic functions that assign a fixed outcome a_i for each measurement, i.e. $D(a_i|x_i, \lambda) = \delta_{a_i, \lambda(x_i)}$, such that $a_i = \lambda(x_i)$, being $\lambda(\cdot)$ a function from $\{0, \ldots, m-1\}$ to $\{0, \ldots, d-1\}$ [BCP+14]. If

we denote by $\vec{D}_\lambda$ the vector associated to a given deterministic strategy $\prod_i D(a_i|x_i,\lambda)$, equation (2.37) tells us that each local point can be expressed as a convex combination of the various $\vec{D}_\lambda$. Those deterministic vectors are the vertices of the local polytope and can be enumerated by counting the number of possible deterministic assignments of the d outputs for each party as a function of m inputs, amounting to $(d)^{mn}$.

From such a characterisation one derives a very general method to detect if a given distribution is local or not. Indeed, this question is equivalent to asking whether a given point $\vec{P}$ can be expressed as a convex combination of the vertices $\vec{D}_\lambda$, which is a feasibility problem that can be addressed with linear programming [ZKBL99, KGanidZ$^+$00]. Although in principle it is possible to derive the local vertices for any Bell scenario, their number grows exponentially with both the number of parties and the number of inputs. Hence, the LP approach to nonlocality detection is actually efficiently implementable only for cases with small values of N and m.

Another useful nonlocality detection tool is provided by the fact that any polytope admits a dual description in terms of a finite set of facets. Those are linear inequalities in terms of the probabilities

$$\mathcal{B} = \sum_{a_1,\ldots a_N} \sum_{x_1,\ldots x_N} \alpha^{a_1,\ldots a_N}_{x_1,\ldots x_N}\, p(a_1,\ldots,a_N|x_1,\ldots,x_N) \geq \beta_C \qquad (2.38)$$

which are satisfied by all local correlations. The facets of $\mathcal{L}$ are usually referred to as *Bell inequalities* and the quantity β_C is termed *local bound*. Geometrically, a Bell inequality is a hyperplane separating the local set from the its complement (cfr. Figure 2.6.a). Importantly, any nonlocal distribution violates at least one Bell inequality, which can be seen again as a consequence of the separating hyperplane theorem. Notice that to define a valid Bell inequality one does not necessarily have to consider a facet of the local polytope (see Figure 2.6.a). However, determining the complete list of local facets provides a sufficient condition for nonlocality detection in a given scenario. Recall that, as mentioned in Section 2.1.1, given the knowledge of the vertices of a polytope, determining its complete list of facets is known as the convex hull problem. For the case of the local polytope, the convex hull problem cannot be solved efficiently for a general scenario, given the exponential scaling of the vertices. Moreover, it has been proven that determining whether a point $\vec{P}$ belongs to $\mathcal{L}$ is in general NP-complete [AIIS04]. Despite no general and efficient nonlocality detection method can be found, many Bell inequalities are known that can detect nonlocal correlations produced by quantum states, including scenarios consisting of an arbitrary number of inputs, outputs or parties [BCP$^+$14].

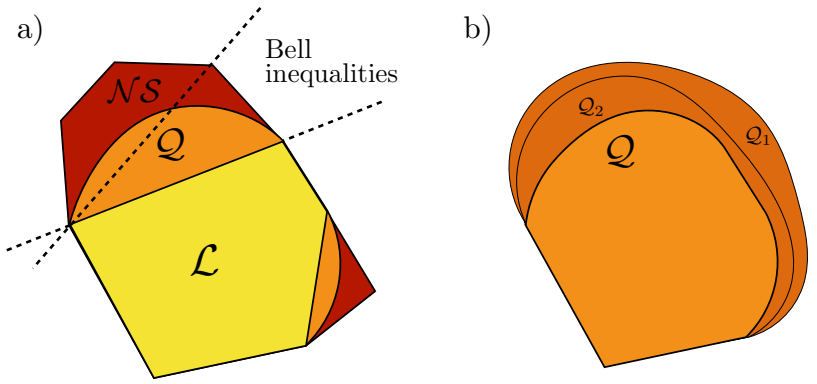

Figure 2.6: a) Schematic bidimensional representation of the sets of local, quantum and no-signalling correlations. As shown in the picture, the three sets are convex and the $\mathcal{L}$ and $\mathcal{NS}$ constitute polytopes. The dotted lines highlights represent examples of Bell inequalities, one of them coinciding with a facet of the local set. b) Pictorial representation of the first two geometrical sets $\mathcal{Q}_\nu$ resulting from the NPA hierarchy and approximating the set of quantum correlations from outside. As shown in the picture $\mathcal{Q}_\nu \subseteq \mathcal{Q}_\mu$ for any $\mu \leq \nu$.

The quantum set

The set of quantum correlations $\mathcal{Q}$ is defined as the set of all vectors $\vec{P}$ that are obtained by the Born rule (2.34) for any choice of POVM measurement operators $M_{x_i}^{a_i}$ and N-partite state ρ. When no restriction is imposed on the dimensions of the local Hilbert spaces $\mathcal{H}_{A_i}$, the set $\mathcal{Q}$ turns out to be convex. Moreover, the state ρ can always be purified and the POVM measurements can be substituted with projectors by means of the Naimark extension [NC02]. In other words, any point in $\mathcal{Q}$ can be obtained as

$$p(a_1, \ldots, a_N | x_1, \ldots, x_N) = \langle \psi | \bigotimes_{i=1}^{N} \Pi_{x_i}^{a_i} | \psi \rangle \tag{2.39}$$

where $|\psi\rangle$ is an arbitrary N-partite pure state in any dimension and the measurement operators $\Pi_{x_i}^{a_i}$ are orthogonal projectors.

Finding a complete way of characterising the quantum set $\mathcal{Q}$ is a very important question that remains still open in general. To date, the most effective method to study the properties of quantum correlations is based on a hierarchy of outer approximations to $\mathcal{Q}$, first introduced in [NPA07, NPA08]. Such a technique, very commonly referred to as Navascués-Pironio-Acín (NPA) hierarchy, is based on the following con-

struction: consider a set $\mathcal{O}$, composed by some products of the measurements operators $\{\Pi_{x_i}^{a_i}\}$ or linear combinations of them. Instead of imposing a tensor product structure as in (2.39), one defines valid measurements operators as those satisfying the following properties

1) $(\Pi_{x_i}^{a_i})^\dagger = \Pi_{x_i}^{(a_i)}$ for any $i = 1, \ldots N$, $x_i = 0, \ldots, m-1$ and $a_i = 0, \ldots, d-1$,

2) $\Pi_{x_i}^{(a_i)}\Pi_{x_i}^{(a_i')} = \delta_{a_i,a_i'}\Pi_{x_i}^{(a_i)}$ for any $i = 1, \ldots N$, $x_i = 0, \ldots, m-1$ and $a_i, a_i' = 0, \ldots, d-1$

3) $[\Pi_{x_i}^{(a_i)}, \Pi_{x_j}^{(a_j)}] = 0$ for any $i \neq j$, $x_i, x_j = 0, \ldots, m-1$ and $a_i, a_j = 0, \ldots, d-1$.

By indexing the elements in the set as $\mathcal{O}_i$ with $i = 1, \ldots k$, we introduce the so-called moment matrix Γ as the $k \times k$ matrix whose entries are defined by $\Gamma_{ij} = tr(\rho\mathcal{O}_i^\dagger\mathcal{O}_j)$. For any choice of measurements and state, it can be shown that Γ satisfies the following properties: i) it is positive semidefinite, ii) its entries satisfy a series of linear constraints associated to the properties 1)-3) of the measurement operators, iii) some of its entries are associated to the observed probability distribution (2.39), iv) some of its entries correspond to unobservable numbers (e.g. when O_i and O_j involve non-commuting observables).

Based on these facts, one can define a hierarchy of tests to check whether a given set of correlations has a quantum realisation. One first defines the sets $\mathcal{O}_\nu$ composed of products of at most ν of the measurement operators, and creates the corresponding Γ matrix using the set of correlations and leaving the unknown entries as variables. Then one seeks for values for these variables that could make the Γ positive semidefinite. This problem constitutes a semidefinite program, hence it can be solved efficiently by numerical methods. Notice that, because of the considerations made above, for any distribution in $\mathcal{Q}$ it is possible to find values that lead to a non-negative moment matrix. However, for a fixed level ν^*, there might be some supra-quantum correlations (i.e. distributions that do not admit any quantum realisations) that are also compatible with a positive semidefinite Γ. It follows that the sets $\mathcal{Q}_\nu$ of points compatible with the SDP test at level ν constitute approximations to the quantum set from outside. By increasing the value of ν, one gets a sequence of stricter and stricter tests and hence better and better approximations to $\mathcal{Q}$ (for a pictorial representation, see Figure 2.6.b).

The NPA hierarchy has been extensively used for various different applications, ranging from the calculation of maximal quantum violations of Bell inequalities to estimating the amount of randomness that

can be achieved in device-independent protocols. It also provides several insights on the geometrical structure of the quantum set itself. Interestingly, it was realised that the SDP hierarchy resulting from NPA is nothing but an application in this context of the more general method for polynomial optimisation over non-commuting variables introduced in [PNA10, DLTW08]. Thus, one can see it as a generalisation of the techniques for commuting variables introduced in Section 2.1.4.

The no-signalling set

From a more fundamental point of view, it is interesting to ask which are the relevant physical principles that constrain the correlations that can be achieved in a Bell scenarios. Clearly, a first unavoidable condition that defines observed probabilities is that any distribution $\vec{P}$ has to be normalised and composed by non-negative numbers, that is

$$p(a_1,\ldots,a_N|x_1,\ldots,x_N) \geq 0\,, \quad \forall\ a_i = 0,\ldots,d-1 \text{ and } x_i = 0,\ldots,m-1 \tag{2.40}$$

and

$$\sum_{a_1,\ldots,a_N} p(a_1,\ldots,a_N|x_1,\ldots,x_N) = 1\,, \quad \forall\ x_i = 0,\ldots,m-1\ . \tag{2.41}$$

Given that the parties are not allowed to communicate during their interaction with the boxes, another natural assumption is the *no-signalling* condition

$$\begin{aligned}\sum_{a_i} \big[&p(a_1,\ldots,a_i,\ldots,a_N|x_1,\ldots,x_i,\ldots,x_N) \\ &-p(a_1,\ldots,a_i,\ldots,a_N|x_1,\ldots,x_i',\ldots,x_N)\big] = 0,\end{aligned} \tag{2.42}$$

for all x_i, x_i', $a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_N$ and $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_N$ and all $i = 1,\ldots,N$. From a physical point of view, it means that the choice of measurement of the i-th party cannot influence the outcome of the remaining measurements. The set $\mathcal{NS}$ of correlations satisfying those three conditions is called the *no-signalling set*. It is easy to see that $\mathcal{NS}$ is also a polytope, since it is defined by a finite amount of linear equalities and inequalities. Moreover, the list of constraints in eqs. (2.40) to (2.42) represents all the facets of the set.

Quantum correlations satisfy normalisation, non-negativity and no-signalling by construction, and hence local correlations as well. However, there are no-signalling correlations that can violate Bell inequalities more than quantum correlations do, meaning that there are probabilities satisfying the non-signalling principle that do not have a quantum representation [PR94]. Therefore, the relations between the three sets introduced in

this section can be summarised as $\mathcal{P} \subset \mathcal{Q} \subset \mathcal{NS}$, where both inclusions are strict (see Figure 2.6.a).

It is also useful to notice that correlations can be equivalently described by a collection of expectation values, also referred to as correlators. For further purposed, let us present them by restricting to case of dichotomic measurements, namely when $d = 2$: in a generic $(N, m, 2)$ scenario, they read as

$$\left\langle M_{x_{i_1}}^{(i_1)} \dots M_{x_{i_k}}^{(i_k)} \right\rangle = \sum_{a_1,\dots,a_N} (-1)^{\sum_{l=1}^{k} a_{i_l}} p(a_1, \dots, a_N | x_1, \dots, x_N) \quad (2.43)$$

with $i_1 < \dots < i_k = 1, \dots, N$, $x_{i_l} = 0, \dots, m-1$ and $k = 1, \dots, N$ (all possible expectation values, ranging from the single-body to N-partite ones are taken into account). The probability and correlator representations are related through the formula

$$p(a_1, \dots, a_N | x_1, \dots, x_N) = \\ \frac{1}{2^N} \left[1 + \sum_{k=1}^{N} \sum_{1 \le i_1 < i_2 < \dots < i_k \le N} (-1)^{\sum_{j=1}^{l} a_{i_j}} \left\langle M_{x_{i_1}}^{(i_1)} \dots M_{x_{i_k}}^{(i_k)} \right\rangle \right], \quad (2.44)$$

where the above equation holds for any $a_i = 0, 1$ and $x_i = 0, \dots, m-1$. Notice also that the equations (2.43,2.44) can be generalised to scenarios with $d > 2$. The main advantage of the correlator picture is that it automatically incorporates the no-signalling and normalisation constraints, thus reducing the number of variables that need to be considered. In particular, this implies that the no-signalling set can be simply described by the conditions of non-negativity of probabilities (2.40), expressed in terms of correlators through (2.44). Notice also that, although we stated all the definitions regarding quantum and local correlations in terms of probabilities, everything can be reformulated in correlator form, by directly applying the Fourier transform (2.44).

Lastly, notice that the number of facets describing $\mathcal{NS}$, i.e. the positivity constraints, grows as $(dm)^N$, which prevents from having an efficient characterisation of the no-signalling set for high values of N, m, d, and especially in multipartite scenarios. In particular, enumerating the no-signalling vertices is generally a hard task, and their complete list is currently known only for few scenarios. Remarkably, they have been completely characterised for the simplest cases of arbitrary number of inputs and outputs, namely in the scenarios $(2, m, 2)$ [JM05, BP05] and $(2, 2, d)$ [BLM$^+$05]. On the contrary, in the multipartite case they can be explicitly computed only in the $(N, 2, 2)$ scenarios and for $N \le 3$ [PBS11].

2.3.3 Multipartite notions of nonlocality

As for the case of entanglement, a relevant question to ask in the multipartite setting is how to quantify the amount of parties that share genuinely nonlocal correlations. Several approaches have been proposed to describe the types of nonlocality that can appear in such a scenario [BBGP09, CGL15]. Following [CGL15], we choose here the notion of k-producibility of nonlocality or nonlocality depth, which goes along the lines developed to describe multipartite entanglement. To this end, recall the definition of an L_k-partition of the set of parties $I = \{1, \ldots, N\}$ into collection of subsets of $\mathcal{A}_l$ of size at most k, introduced in Section 2.2.3. Consider now correlations that admit the following decomposition

$$p(a_1, \ldots, a_N|x_1, \ldots, x_N) = \sum_{\lambda} p(\lambda) p_1(\mathbf{a}_{\mathcal{A}_1}|\mathbf{x}_{\mathcal{A}_1}, \lambda) \cdot \ldots \cdot p_L(\mathbf{a}_{\mathcal{A}_L}|\mathbf{x}_{\mathcal{A}_L}, \lambda) \tag{2.45}$$

where $\mathbf{a}_{\mathcal{A}_i}$ and $\mathbf{x}_{\mathcal{A}_i}$ are vectors encoding the outcomes and measurements choices corresponding to the observers belonging to $\mathcal{A}_i$. One can see that this is a natural generalisation of the notion of L_k-separable states (2.26) to the device-independent framework.

Still, the form of correlations (2.45) is not yet the most general one as mixtures of different L_k-partitions do not increase the nonlocality depth of the resulting probability distribution. We then call correlations $\{p(\mathbf{a}|\mathbf{x})\}$ *k-producible* if they can be written as a convex combination of correlations that are k-producible with respect to different L_k-partitions, i.e.,

$$p(a_1, \ldots, a_N|x_1, \ldots, x_N) = \sum_{S \in S_k} q_S p_S(a_1, \ldots, a_N|x_1, \ldots, x_N) \tag{2.46}$$

where S_k is the set of all L_k-partitions and $p_S(a_1, \ldots, a_N|x_1, \ldots, x_N)$ are correlations that admit the decomposition (2.45) with respect to the k-partition S.

Similarly to the connection between separable states and local correlations, it is easy to see from (2.27) that correlations produced by applying local measurements on k-separable states are always k-producible. Moreover, they admit a decomposition where correlations shared among subgroups have quantum realisation by definition. Hence, ruling out a k-producible description with quantum resources, i.e. with $p_i(\mathbf{a}_{\mathcal{A}_i}|\mathbf{x}_{\mathcal{A}_i}, \lambda) \in \mathcal{Q}$ can be seen as a device-independent method to detect a given entanglement depth. However, given the absence of an exact characterisation of the quantum set, techniques that approach k-producible correlations with quantum nonlocal resources are currenlty based on numerical approximations [BGLP11, LRB$^+$15, MBL$^+$13].

A sometimes more convenient choice to study k-producible models is to allow for no-signalling resources, that is, to require the distributions $p_i(\mathbf{a}_{\mathcal{A}_i}|\mathbf{x}_{\mathcal{A}_i}, \lambda)$ to satisfy the no-signalling condition (2.42). More general resources can also be considered, but some of them are known to lead to self-contradicting models while others can not easily be generalised to partitions of size larger than 2 [GWAN12, BBGP13]. By taking the no-signalling picture, we define the minimal k for which a distribution can be expressed in the form (2.46) as its *nonlocality depth* k. Equivalently, correlations whose nonlocality depth is k are generally referred to as *genuinely k-partite nonlocal* or, simply, *k-nonlocal* [Sve87]. Let us notice that in the particular case of $k = 1$, where each party forms a singleton $\mathcal{A}_i = \{A_i\}$ $(i = 1, \ldots, N)$, one recovers the definition of local correlations (2.35). Then, on the other extreme $k = N$, we have correlations in which all parties share nonlocality and are thus called *genuinely multipartite nonlocal* (GMNL).

Geometrically, the choice of no-signalling resources makes the k-producible correlations form polytopes, denoted $\mathcal{P}_{N,k}$. Similarly to the local polytope, vertices of these polytopes are product probability distributions of the form

$$p(\mathbf{a}|\mathbf{x}) = p_1(\mathbf{a}_{\mathcal{A}_1}|\mathbf{x}_{\mathcal{A}_1}) \cdot \ldots \cdot p_L(\mathbf{a}_{\mathcal{A}_L}|\mathbf{x}_{\mathcal{A}_L}) \tag{2.47}$$

with each $p_i(\mathbf{a}_{\mathcal{A}_i}|\mathbf{x}_{\mathcal{A}_i})$ being a vertex of the corresponding $|\mathcal{A}_i|$-partite $\mathcal{NS}$ polytope (when $|\mathcal{A}_i| = 1$, then $p_i(\mathbf{a}_{\mathcal{A}_i}|\mathbf{x})$ is simply a deterministic vertex of the local polytope). It thus follows that the necessary ingredient in order to construct all vertices of $\mathcal{P}_{N,k}$ are the vertices of the p-partite nonsignaling polytopes $\mathcal{NS}_p$ for all $p \leq k$, which is in general a very demanding task. The facets constraining the $\mathcal{P}_{N,k}$ polytopes can also be interpreted as Bell-like inequalities. In this case, the violation of such inequalities implies that a given distribution cannot be described by any k-producible model. Hence, such inequalities are used to certify that the correlations violating them are at least $(k + 1)$-nonlocal.

Despite the complexity of the problem prevents a complete characterisation of the k-producible polytopes, many advancements have been made in the context of deriving specific families of Bell inequalities. Apart from considering inequalities that detect GMNL [Sve87, BBGL11], recent efforts resulted in the construction of inequalities detecting a given nonlocality depth k [CGL15] or calculation of k-producible bounds (i.e. the maximal value β_k achiveable with correlations $\mathcal{P}_{N,k}$) for already known Bell inequalities [BBGP09, LRB$^+$15]. In such a way, one can estimate the nonlocality depth by simply looking at the amount of the observed inequality violation.

Lastly, notice that, with the aid of the formula (2.44), all the above

definitions can be equivalently formulated in terms of correlators (2.43); in particular, for a vertex the correlators (2.43) factorise whenever the parties belong to different groups $\mathcal{A}_i$.

2.3.4 Self-testing

Another relevant application of nonlocality is self-testing, first introduced in [MY04], which can be seen as the most complete form of certifying the quantum properties of a given system. Indeed, the aim of self-testing is to completely characterise (up to uncontrollable symmetries) the state that has been prepared and/or the measurement performed by simply looking at the resulting probability distribution. Such a tool is particularly interesting because it offers a way to guarantee that a given quantum device is working properly without having to know the details of its internal functioning, that is, in a device-independent way.

Self-testing is an interesting problem also from a fundamental point of view and it can give important insights on the structure of the set of quantum correlations. Geometrically, the fact that some correlation can be uniquely related to a given state and measurements raises the question of which properties of the points in $\mathcal{Q}$ identify them as correlations that can be associated to a self-testing statement. A clear necessary condition is for a point to be extremal, that is, not to be decomposable as a convex combination of other vectors in the set. A feature that is known to be sometimes sufficient for self-testing is to exploit the fact that some correlations violate maximally a Bell inequality [MY04, ŠASA16, BP15]. However, there are also self-testing proofs that are based on the knowledge of the whole probability distribution or parts of it [CGS17, McK11, ŠCAA18]. Moreover, there is evidence that for some points of the quantum set, the maximal violation of a single Bell inequality is not enough to identify their extremality [GKW$^+$18]. From a more applied point of view, a relevant question is to classify the quantum states that can be self-tested. While in the bipartite case it is known that all states can be [CGS17], in the multipartite scenario the problem is still open.

For the purposes of this thesis, we focus on the methods of state and measurements self-testing based on the maximal violation of a Bell inequality. Suppose then that one is interested in certifying a *target state* $|\psi\rangle$ and some *target measurements* $\{M_{x_i}^{a_i}\}_{x_i=0,\dots,m-1}^{a_i=0,\dots,d-1}$ for parties $i = 1,\dots,N$. Assume also that the resulting probability distribution achieves the violation β_Q for a given Bell inequality $\mathcal{B}$ of the form (2.38). A first crucial step is to prove that such violation is indeed the maximal value that can be obtained by quantum theory. To do so, one has to show that

the maximal eigenvalue of the corresponding Bell operator

$$\hat{\mathcal{B}} = \sum_{a_1,\dots a_N} \sum_{x_1,\dots x_N} \alpha^{a_1,\dots a_N}_{x_1,\dots x_N} \Pi^{a_1}_{x_1} \otimes \dots \otimes \Pi^{a_N}_{x_N} \tag{2.48}$$

is bounded by β_Q for any choice of local projectors $\Pi^{a_i}_{x_i}$ in any Hilbert space dimension. In other words, the shifted Bell operator $(\beta_Q \mathbb{1} - \hat{\mathcal{B}})$ has to be positive semidefinite.

A very common way to prove that is to show that such operator is a *sum of squares* (SOS), that is

$$(\beta_Q \mathbb{1} - \hat{\mathcal{B}}) = \sum_k \mathcal{P}_k^\dagger \mathcal{P}_k \tag{2.49}$$

where the $\mathcal{P}_k$ are polynomials in the $\Pi^{a_i}_{x_i}$ variables. Indeed, any operator of the form $\mathcal{P}_k^\dagger \mathcal{P}_k$ is non-negative by construction and the condition (2.49) directly implies that $\mathrm{tr}\,(\hat{\mathcal{B}}\rho) \leq \beta_Q$ for any choice of quantum state and measurements.

Let us assume that one has observed some correlations obtaining a violation β_Q for the inequality $\mathcal{B}$, produced by an unknown *physical state* $|\psi\rangle$ (recall that in a device-independent framework the state can always be assumed to be pure) and some unknown measurements $\{N^{a_i}_{x_i}\}^{a_i=0,\dots,d-1}_{x_i=0,\dots,m-1}$ for parties $i = 1, \dots, N$. A self-testing statement consists in showing that there exists a *local isometry* $\Phi = \Phi_1 \otimes \dots \Phi_N$ connecting the physical and the target state, namely

$$\Phi\left[|\phi\rangle\right] = |\psi\rangle \otimes |\mathrm{aux}\rangle \tag{2.50}$$

and similarly for the measurements

$$\Phi\left[(N^{a_1}_{x_1} \otimes \dots N^{a_N}_{x_N})\,|\phi\rangle\right] = (M^{a_1}_{x_1} \otimes \dots M^{a_N}_{x_N})\,|\psi\rangle \otimes |\mathrm{aux}\rangle \tag{2.51}$$

where $|\mathrm{aux}\rangle$ is some state encoding uncorrelated degrees of freedom and the second equation holds for all $a_i = 0, \dots, d-1$ and $x_i = 0, \dots, m-1$. The physical interpretation of equations (2.50) and (2.51) is that the physical state and measurements are indeed equivalent to the target ones, up to some uncontrollable operations (the local isometries) that do not change the resulting probability distribution. Notice that here we are assuming that both the target state and measurements are real, since otherwise they could not be distinguished from their complex conjugates by looking at the correlations only.

For further purposes, we focus on a Bell inequality-based approach to self-testing where the local isometry is constructed exploiting the conditions resulting from the SOS decomposition of the shifted Bell operator.

More precisely, notice that applying the operator (2.49) on a state $|\phi\rangle$ maximally violating the inequality $\mathcal{B}$ gives exactly zero, which directly implies the set of condition $\mathcal{P}_k |\phi\rangle = 0$ for all terms in the decomposition. As we will see in an example in the next section, those equations are sometimes enough to make a self-testing statement for both the state and the measurements.

Lastly, let us stress that in order to apply self-testing protocols in practical situations, one is actually interested in a more quantitative statement than those provided by equation (2.50) and (2.51). In particular, it is for instance more convenient to be able to bound the fidelity between the target and the physical state

$$\Theta(\phi \to \psi) = \max_{\Phi_1,\ldots,\Phi_N} |\langle\psi| \left[(\Phi_1 \otimes \ldots \otimes \Phi_N) |\phi\rangle\right]|^2 \tag{2.52}$$

as a function of the observed Bell inequality violation β_{obs}, also in cases where it is not maximal. Here we revise a useful technique to obtain such bounds, first introduced in [Kan16]. For this purpose, we notice that the fidelity in (2.52) can equivalently be written as

$$\langle\phi| \left[(\Phi_1^\dagger \otimes \ldots \otimes \Phi_N^\dagger)(|\psi\rangle\ \langle\psi|)\right] |\phi\rangle \tag{2.53}$$

where $\Phi_i^\dagger$ are dual maps of the quantum channels Φ_i. Now, proving for some particular channels Φ_i an operator inequality

$$K := (\Phi_1^\dagger \otimes \ldots \otimes \Phi_N^\dagger)(|\psi\rangle\ \langle\psi|) \geq s\hat{\mathcal{B}} + \mu\mathbb{1} \tag{2.54}$$

with for some $s, \mu \in \mathbb{R}$, where $\hat{\mathcal{B}}$ is constructed from any possible local observables, would imply the following inequality for the fidelity

$$\Theta(\phi \to \psi) \geq s\beta_{obs} + \mu. \tag{2.55}$$

Proving an operator inequality (2.54) for arbitrary local observables in $\hat{\mathcal{B}}$ is certainly a formidable task. However, (2.55) provides a simple bound that can at least be estimated numerically and even proven analytically for some of the simplest Bell scenarios and corresponding inequalities.

2.3.5 A simple example: CHSH

Let us study in more detail the simplest Bell scenario, namely the $N = m = d = 2$ case. For convenience we call the two parties Alice and Bob, denote their projectors M_x^a and N_y^b with $x, y, a, b = 0, 1$ and adopt the correlators picture, denoting by $A_x = M_x^1 - M_x^0$ and $B_y = N_y^1 - N_y^0$ the corresponding hermitian operators. Notice that in such a dichotomic

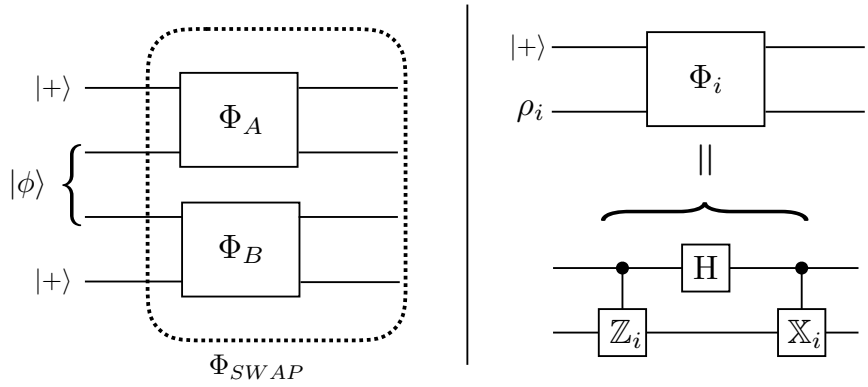

Figure 2.7: A circuit representation of the SWAP isometry. The isometry can be viewed as a unitary with each branch acting on the i-th particle of $|\phi\rangle$ and one ancillary qubit in the state $|+\rangle$. On the right-hand-side, the explicit form of each of the two unitaries Φ_A and Φ_B, constructed as a function of the local operators $\mathbb{X}_i, \mathbb{Z}_i$.

measurement scenario, those operators always square to identity, that is $A_x^2 = B_y^2 = \mathbb{1}$ for all $x, y = 0, 1$. In the considered scenario, a very well-known Bell inequality is the Clauser-Horne-Shimony-Holt (CHSH) [CHSH69], which reads

$$\mathcal{B}_{CHSH} = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2\,, \tag{2.56}$$

where recall that the two-body correlators are defined as $\langle A_x B_y \rangle = p(a = b|xy) - p(a \neq b|xy)$. Interestingly, it can be shown that CHSH is the only relevant Bell inequality in the considered scenario, that is, all the facets of the local polytope correspond to (2.56) up to relabellings of parties, inputs and outputs.

The maximal quantum violation of CHSH amounts to $\beta_Q = 2\sqrt{2}$ and it is achieved by the maximally entangled two-qubit state $|\phi^+\rangle$ and with Alice's and Bob's measurements being $A_x = (X + (-1)^x Z)/\sqrt{2}$ and $B_0 = X, B_1 = Z$ respectively. The fact that no value higher than $2\sqrt{2}$ can be achieved by quantum theory can be proved by writing the following SOS decomposition

$$\begin{aligned}(2\sqrt{2}\mathbb{1} - \mathcal{B}_{CHSH}) \;&=\; \frac{1}{\sqrt{2}}\left[\mathbb{1} - \frac{A_0 + A_1}{\sqrt{2}} B_0\right]^2 \\ &\quad + \frac{1}{\sqrt{2}}\left[\mathbb{1} - \frac{A_0 - A_1}{\sqrt{2}} B_1\right]^2 \end{aligned} \tag{2.57}$$

We notice that when acting on the state $|\phi\rangle$ maximally violating the CHSH inequality, the right-hand-side of (2.57) must vanish. Therefore, if we define the following operators

$$\mathbb{X}_A = \frac{A_0 + A_1}{2}\,, \quad \mathbb{Z}_A = \frac{A_0 - A_1}{2}\,, \tag{2.58}$$

$$\mathbb{X}_B = B_0 \quad \mathbb{Z}_B = B_1\,. \tag{2.59}$$

the following conditions hold

$$\begin{aligned} (\mathbb{Z}_B - \mathbb{Z}_A)\,|\phi\rangle = 0\,, \\ (\mathbb{X}_B - \mathbb{X}_A)\,|\phi\rangle = 0\,. \end{aligned} \tag{2.60}$$

Moreover, $\{\mathbb{X}_A, \mathbb{Z}_A\} = 0$ holds by construction of the operators, which, combined with (2.60) implies that $\mathbb{X}_B$ and $\mathbb{Z}_B$, when applied on $|\phi\rangle$, anticommute as well. Similarly, Bob's operators satisfy $\mathbb{X}_B^2 = \mathbb{Z}_B^2 = \mathbb{1}$, hence Alice's ones square to identity when acting on $|\phi\rangle$. Now, as a last step to prove that the maximal violation of CHSH self-tests the maximally entangled two-qubit state, we apply the SWAP gate [MYS12] (represented in Figure 2.7)

$$\begin{aligned} \Phi_{SWAP}(|\phi\rangle\,|+\rangle^{\otimes 2}) \;=\; & \mathbb{Z}_A^+\mathbb{Z}_B^+\,|\phi\rangle\,|00\rangle + \mathbb{Z}_A^+\mathbb{X}_B\mathbb{Z}_B^-\,|\phi\rangle\,|01\rangle \\ & + \mathbb{X}_A\mathbb{Z}_A^-\mathbb{Z}_B^+\,|\phi\rangle\,|10\rangle + \mathbb{X}_A\mathbb{Z}_A^-\mathbb{X}_B\mathbb{Z}_B^-\,|\phi\rangle\,|11\rangle \end{aligned} \tag{2.61}$$

where we have defined the two orthogonal projectors $\mathbb{Z}_i^{\pm} = \frac{\mathbb{1}\pm\mathbb{Z}_i}{2}$. Then, by making use of the properties (2.60), we first notice that the second term in the sum vanishes, indeed

$$\mathbb{Z}_A^+\mathbb{X}_B\mathbb{Z}_B^-\,|\phi\rangle\,|01\rangle = \mathbb{Z}_A^+\mathbb{Z}_A^-\mathbb{X}_B\,|\phi\rangle\,|01\rangle = 0 \tag{2.62}$$

and, by applying the same argument, the third term is zero as well. To conclude, we focus on the last term, which becomes

$$\begin{aligned} & \mathbb{X}_A\mathbb{Z}_A^-\mathbb{X}_B\mathbb{Z}_B^-\,|\phi\rangle\,|11\rangle = \mathbb{X}_A\mathbb{Z}_A^-\mathbb{Z}_B^+\mathbb{X}_B\,|\phi\rangle\,|11\rangle \\ & = \mathbb{X}_A\mathbb{Z}_A^-\mathbb{Z}_B^+\mathbb{X}_A\,|\phi\rangle\,|11\rangle = \mathbb{Z}_A^+\mathbb{Z}_B^+\,|\phi\rangle\,|11\rangle \end{aligned} \tag{2.63}$$

where we have also used that $\mathbb{X}_A^2\,|\phi\rangle = |\phi\rangle$. This concludes the proof, since we have shown that there is an isometry connecting $|\phi\rangle$ with the maximally entangled state, namely

$$\Phi_{SWAP}(|\phi\rangle\,|+\rangle^{\otimes 2}) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |\text{aux}\rangle \tag{2.64}$$

where $|\text{aux}\rangle = \sqrt{2}\mathbb{Z}_A^+\mathbb{Z}_B^+ |\psi\rangle$. By using a similar argument, it is also possible to show that

$$\Phi_{SWAP}((A_x \otimes B_0) |\phi\rangle \otimes |00\rangle) = \left(\frac{(X + (-1)^x Z)}{2} \otimes X\right) \left|\phi^+\right\rangle \otimes |\text{aux}\rangle \ ,$$
$$\Phi_{SWAP}((A_x \otimes B_1) |\phi\rangle \otimes |00\rangle) = \left(\frac{(X + (-1)^x Z)}{2} \otimes Z\right) \left|\phi^+\right\rangle \otimes |\text{aux}\rangle \ . \tag{2.65}$$

Chapter 3

Efficient Device-Independent Entanglement Detection for Multipartite Systems

Entanglement is one of the most studied properties of quantum mechanics for its application in quantum information protocols. Nevertheless, detecting its presence in large multipartite states continues to be a great challenge both from the theoretical and the experimental point of view. Most of the known methods either have computational costs that scale inefficiently with the number of particles or require more information on the state than what is attainable in everyday experiments. In this Chapter we introduce a new technique for entanglement detection that provides several important advantages in these respects. First, it scales efficiently with the number of particles, thus allowing for application to systems composed by up to few tens of particles. Second, it needs only the knowledge of a subset of all possible measurements on the state, therefore being apt for experimental implementation. Moreover, since it is based on the detection of nonlocality, our method is device independent. We report several examples of its implementation for well-known multipartite states, showing that the introduced technique has a promising range of applications. The results of this Chapter are based on the original work published in [BCWA17].

3.1 Introduction

As we argued in Section 2.2, entanglement is the key ingredient for several quantum information protocols. Hence, developing techniques to detect its presence in quantum states is a task of crucial importance that has

attracted a lot of research effort.

Recall that the most general way to detect entanglement in a given system consists of reconstructing its quantum state using tomography and then applying any entanglement criterion to the resulting state. This, however, is costly both from an experimental and a theoretical perspective. First, determining the state of large quantum systems is impractical in experiments, given that quantum tomography implies measuring a number of observables that increases exponentially with the number of systems, e.g., 3^N observables even in the simplest case of N qubits [HHR$^+$05]. Second, determining whether an arbitrary state is entangled is known to be a hard problem – the computational resources of the most efficient known algorithm, namely the symmetric extension, scale exponentially with N [BC12]. Because of these problems, it is very desirable to develop entanglement detection techniques with more accessible experimental and computational requirements.

One possible approach is to make use of entanglement witnesses. Recall that these are criteria for detecting entanglement that require measuring only some expectation values of local observables. In particular, attempts have been made to derive witnesses that adapt to the limited amount of information that is usually available in a typical experiment. For instance, one can consider witnesses involving only two-body correlators [TG06] or a few global measurements [LPV$^+$14, VAET14]. Nonetheless, entanglement witnesses constitute a method that lacks generality, given that the known methods are generally tailored to detect very specific states. There are techniques capable of deriving a witness for any generic entangled state, which can also be constrained to the available set of data [JMG11], or adapted to require the minimal amount of measurements on the system [KSK$^+$16]. However, they always involve an optimisation procedure that runs on an exponentially increasing number of parameters. A method to detect metrologically useful (hence entangled) states based on a couple of measurements has recently been proposed [AKGT17]. However, these states represent only a subset of all entangled states.

A qualitatively different approach to entanglement detection is based on Bell nonlocality (cfr. Section 2.3). Indeed, the presence of nonlocality provides a certificate of the entanglement in the state. Moreover, it has the advantage that it can be assessed in a device-independent manner, i.e. without making any assumption on the actual experimental implementation. The easiest way to detect nonlocality is by means of the violation of a Bell inequality. However, in analogy with the entanglement case, each inequality is usually violated by a very specific class of states. In the general case, verifying whether a set of observed correlations is nonlocal

can be done via linear programming. Nonetheless, the number of variables involved again grows exponentially with the number of particles, e.g. as 4^N already for the simplest scenarios where only two dichotomic measurements per party are applied.

To summarise, the methods to detect entanglement known so far are either not general or too costly, from a computational and/or experimental viewpoint, to be applied to large systems.

In this Chapter we present a novel technique for device-independent entanglement detection that is efficient both experimentally and computationally. On the one hand, it requires the knowledge of a subset of all possible measurements, most of them consisting of few-body correlation functions, which makes it suitable for practical implementations. On the other hand, it can be applied to any set of observed correlations and can be implemented by semidefinite programming involving a number of variables that grows polynomially with N.

Of course, all these nice properties become possible only because our method for entanglement detection is a relaxation of the initial hard problem. However, and despite being a relaxation, we demonstrate the power of our approach by showing how it can be successfully applied to several physically relevant examples for systems of up to 29 qubits.

3.2 Relaxing the nonlocality detection problem

Recall that in a general (N, m, d) Bell scenario we have N observers sharing a multipartite quantum state ρ, each performing one out of m possible local measurements $M_{x_i}^{a_i}$, where $x_i = \{0, \ldots, m-1\}$ and $a_i = \{0, \ldots, d-1\}$. The object of interest is the resulting probability distribution

$$p(a_1, \ldots, a_N | x_1, \ldots, x_N) = \mathrm{tr}\left(M_{x_1}^{a_1} \otimes M_{x_N}^{a_N} \rho\right), \tag{3.1}$$

which can be estimated by performing the presented experiment sufficiently many times. Since in the following we often restrict our considerations to dichotomic measurements, it is convenient to adopt the correlator picture: recall from their definition (2.43), which we rewrite as

$$\langle M_{x_{i_1}}^{(i_1)} \ldots M_{x_{i_k}}^{(i_k)} \rangle = \sum_{a_{i_1}, \ldots, a_{i_k}} (-1)^{\sum_{l=1}^{k} a_{i_l}} p(a_{i_1} \ldots, a_{i_k} | x_{i_1}, \ldots, x_{i_k}) \tag{3.2}$$

where $0 \leq i_1 < \ldots < i_k < N$, $x_{i_j} \in \{0, m-1\}$ and $1 \leq k \leq N$ and we have defined the marginal distributions

$$p(a_{i_1}, \ldots, a_{i_k} | x_{i_1}, \ldots x_{i_k}) = \mathrm{tr}(M_{x_{i_1}}^{a_{i_1}} \otimes \ldots \otimes M_{x_{i_k}}^{a_{i_k}} \rho_{i_1, \ldots, i_k}) \tag{3.3}$$

where $0 \leq i_1 < \ldots < i_k < N$, $1 \leq k \leq N$ and $\rho_{i_1,\ldots,i_k}$ is the reduced state of ρ_N corresponding to the considered subset of parties. Notice that marginals can equivalently be obtained from the full distribution (3.1) by summing over the remaining outcomes. The value of k represents the order of the correlators: for instance, expectation values $\langle M_{x_{i_1}}^{(i_1)} M_{x_{i_2}}^{(i_2)} \rangle$ are of order two. Correlators of order N are often referred to as full-body correlators. In scenarios involving only dichotomic measurements, correlators encode all the information in the observed distribution. When working with correlators, it is also useful to introduce the measurement operators in the expectation value form, namely by using the notation $M_{x_i}^{(i)} = M_{x_i}^1 - M_{x_i}^0$. With this definition, it is easy to see that

$$\langle M_{x_{i_1}}^{(i_1)} \ldots M_{x_{i_k}}^{(i_k)} \rangle = \mathrm{tr}\,(M_{x_{i_1}}^{(i_1)} \otimes \ldots \otimes M_{x_{i_k}}^{(i_k)} \rho_{i_1,\ldots,i_k}). \tag{3.4}$$

As explained in Section 2.3, nonlocal correlations can be produced only by entangled states. Here, we will precisely be interested in studying nonlocality as a device-independent entanglement detection method. In particular, in the following Section we will present a relaxation of the nonlocality detection problem and show how it defines a general and efficient method to check if a given state is entangled.

3.2.1 The SDP method

Our method is based on the following reasoning (discussed in detail below):

1. If a quantum state ρ_N is separable, local measurements performed on it produce local correlations (i.e. correlations admitting a local model).

2. Any local correlations can be realised by performing commuting local measurements on a quantum state.

3. Correlations produced by commuting local measurements define a positive moment matrix with constraints associated to the commutation of all the measurements.

4. Our method consists in checking if the observed correlations are consistent with such a positive moment matrix. In the negative case the state ρ_N producing the correlations is proven to be entangled.

Let us now explain all these points in detail. First, recall from Section 2.3.1 that, given a separable quantum state (2.25), any set of conditional probability distributions obtained after performing local measurements

on it admits a decomposition in terms of a LHV model (2.35). By this reasoning, whenever the set of observed distributions (3.1) is nonlocal, we can conclude that the shared state is entangled. Moreover, since nonlocality is a property that can be assessed at the level of the probability distribution, it can be seen as a device-independent way of detecting entanglement. For the sake of brevity, throughout the rest of the paper we therefore refer to our method as a nonlocality detection one.

The second ingredient is that any local set of probability distributions has a quantum realisation in terms of local *commuting measurements* applied to a quantum state [Fin82]. In order to see it more explicitly, recall that any local distribution can be rewritten as a convex combination of deterministic strategies, namely

$$p(a_1,\ldots,a_N|x_1,\ldots,x_N) = \sum_{\lambda} q_\lambda \prod_{i=1}^{N} D(a_i|x_i,\lambda) \tag{3.5}$$

where $D(a_i|x_i,\lambda)$ are deterministic functions that give a fixed outcome a for each measurement. It is easy to see that any such decomposition can be reproduced by choosing the multipartite state $\rho = \sum_\lambda q_\lambda |\lambda\rangle\langle\lambda|^{\otimes N}$ and measurement operators of the form $M_{x_i}^{a_i} = \sum_{\lambda'} D(a_i|x_i,\lambda')|\lambda'\rangle\langle\lambda'|$. In particular, $[M_{x_i}^{(i)}, M_{x_i'}^{(i)}] = 0 \;\forall\; i, x_i$, and x_i'.

The last step consists in using a modified version of the NPA hierarchy (cfr. Section 2.3.2), that takes into account the commutativity of the local measurements to test if the observed probability distribution is local (a similar idea was introduced in the context of quantum steering [KSC$^+$15] – see also [CS17]). The NPA hierarchy consists of a sequence of tests aimed at certifying if a given set of probability distributions has a quantum realisation (3.1). In NPA one imposes the commutativity of the measurements between the distant parties. Now, we impose the extra constraints that the local measurements on each party also commute.

The resulting SDP hierarchy is nothing but an application in this context of the more general method for polynomial optimisation over noncommuting variables introduced in [PNA10], see also [DLTW08]. As we stressed in Section 2.3.2, by imposing commutativity of all the variables this general hierarchy reduces to the well-known Lasserre hierarchy, namely the relaxation for polynomial optimisation of commuting variables presented in Section 2.1.4. Indeed, an alternative interpretation of our method can be found by connecting it to the moment problem, which is at the hearth of Lasserre's relaxation. More precisely, as proven by Fine in [Fin82], a set of correlation is local if and only if it can be reproduced by a joint probability distribution involving all the local measurements (including pairs of potentially incompatible ones). Hence, the

SDP relaxation we propose can be seen as an instance of the truncated moment problem (cfr. Section 2.1.4), namely as a test of compatibility of the observed moments, in the variables $M_{x_i}^{(i)}$, with a joint probability distribution. Let us also mention that a use of this relaxation technique to describe local correlations was also proposed in [SG11]. However, to the best of our knowledge, no systematic analysis of its application to multipartite scenarios has been considered thus far.

3.2.2 Details and convergence of the hierarchy

It is convenient for what follows to recall the main ingredients of the NPA hierarchy. Consider a set $\mathcal{O}$, composed by some products of the measurements operators $\{M_{x_i}^{a_i}\}$ or linear combinations of them. By indexing the elements in the set as $\mathcal{O}_i$ with $i = 1, \ldots k$, we introduce the so-called moment matrix Γ as the $k \times k$ matrix whose entries are defined by $\Gamma_{ij} = tr(\rho_N \mathcal{O}_i^\dagger \mathcal{O}_j)$. For any choice of measurements and state, it can be shown that Γ satisfies the following properties: i) it is positive semidefinite, ii) its entries satisfy a series of linear constraints associated to the commutation relations among measurement operators by different parties and the fact that they correspond to projectors, iii) some of its entries can be computed from the observed probability distribution (3.1), iv) some of its entries correspond to unobservable numbers (e.g. when O_i and O_j involve noncommuting observables).

Based on these facts one can define a hierarchy of tests to check whether a given set of correlations has a quantum realisation. One first defines the sets $\mathcal{O}_\nu$ composed of products of at most ν of the measurement operators, and creates the corresponding Γ matrix using the set of correlations and leaving the unassigned entries as variables. Then one seeks for values for these variables that could make the Γ positive. This problem constitutes a SDP, hence it can be efficiently solved numerically. If no such values are found this means that the set of correlations used does not have a quantum realisation. By increasing the value of ν, one gets a sequence of stricter and stricter ways of testing the belonging of a distribution to the quantum set.

We can now use the same idea to define a hierarchy of conditions to test whether a given set of correlations has a quantum realisation with commuting measurements. To do so we simply impose additional linear constraints on the entries of the moment matrix resulting from assuming that the local measurements also commute (for a more detailed discussion, see Appendix A.1). Thus, given a set of observed probability distributions one can use them to build an NPA-type matrix with the additional linear constraints associated to the local commutation relations, and run an

SDP to check its positivity to certify if the considered set of correlations can not be obtained by measuring a separable state.

Interestingly, the convergence of this hierarchy follows from the results in [NPA08, PNA10]. Roughly speaking, one can say that since the NPA hierarchy is proven to converge to the set of quantum correlations, our method provides a hierarchy that converges to the set of quantum correlations with commuting measurements, which we have shown to be equivalent to the set of local correlations [1]. Therefore, any nonlocal correlation would fail the SDP test at a finite step of the sequence given by the $\mathcal{O}_\nu$.

Moreover, the commutativity of all the measurements implies that the total number of variables that can be involved in the SDP test is finite. The reason is that the longest non-trivial product of the operators that can appear in the moment matrix consists of the products of all the different $M_{x_i}^{a_i}$. Hence, the number of variables in the moment matrix stops growing after the first step at which this product appears. This also implies that the convergence of the hierarchy is met at a finite step as well, namely coinciding to the level ν' at which the longest non-trivial products appear in the list of operators $\mathcal{O}_{\nu'}$. Indeed, it is easy to see that for $\mu > \nu'$, there cannot appear new operators in the generating set, i.e. $\mathcal{O}_\mu = \mathcal{O}_{\nu'}$. Of course, the aforementioned levels depend on the numbers (N, m, d) defining the scenario and it is, in general, high. Indeed, according to the Collins-Gisin representation [CG04], one has $Nm(d-1)$ independent measurement operators $M_{x_i}^{a_i}$. Therefore, the product of all of them would first appear in the moment matrix at level $\lceil \frac{Nm(d-1)}{2} \rceil$. Consequently, convergence is assured at level $\nu' = Nm(d-1)$.

To conclude, we stress that, depending on the level of the hierarchy, one might not need knowledge of the full probability distribution. Indeed, by looking at (3.3), it is evident that to define a marginal distribution involving k parties, one requires the product of k measurements $M_{x_i}^{a_i}$. Now, given that the operators of the set $\mathcal{O}_\nu$ contain products of at most ν measurement operators, the terms in the moment matrix at level ν can only coincide with the marginals of the observed distribution of up to $k = 2\nu$ parties. Therefore, in the multipartite setting, fixing the level of the hierarchy is also a way to limit the order of the marginals that can be assigned in the moment matrix.

[1] A more formal way to see it is to notice that we are restricting the projective algebra of NPA by the commutation condition. Then, given that the original algebra already meets the Archimedean condition, the convergence holds for the commuting case as well.

3.2.3 Simple example

After presenting the general idea of the method, it is convenient to illustrate it with a concrete example. In what follows, we present the explicit form of the moment matrix for the bipartite case, two dichotomic measurements per party and level $\nu = 2$ of the hierarchy. For the sake of simplicity, we rename the expectation value operators for the two parties as $\mathcal{A}_x$ and $\mathcal{B}_y$, with $x, y = 0, 1$. In this scenario, the set of operators reads as $\mathcal{O}_2 = \{\mathbb{1}, \mathcal{A}_0, \mathcal{A}_1, \mathcal{B}_0, \mathcal{B}_1, \mathcal{A}_0\mathcal{A}_1, \mathcal{A}_0\mathcal{B}_0, \mathcal{A}_0\mathcal{B}_1, \mathcal{A}_1\mathcal{B}_0, \mathcal{A}_1\mathcal{B}_1, \mathcal{B}_0\mathcal{B}_1\}$. The corresponding moment matrix is

$$\Gamma = \begin{pmatrix}
1 & \langle\mathcal{A}_0\rangle & \langle\mathcal{A}_1\rangle & \langle\mathcal{B}_0\rangle & \langle\mathcal{B}_1\rangle & v_1 & \langle\mathcal{A}_0\mathcal{B}_0\rangle & \langle\mathcal{A}_0\mathcal{B}_1\rangle & \langle\mathcal{A}_1\mathcal{B}_0\rangle & \langle\mathcal{A}_1\mathcal{B}_1\rangle & v_2 \\
\langle\mathcal{A}_0\rangle & 1 & v_1 & \langle\mathcal{A}_0\mathcal{B}_0\rangle & \langle\mathcal{A}_0\mathcal{B}_1\rangle & \langle\mathcal{A}_1\rangle & \langle\mathcal{B}_0\rangle & \langle\mathcal{B}_1\rangle & v_3 & v_4 & v_5 \\
\langle\mathcal{A}_1\rangle & v_1^* & 1 & \langle\mathcal{A}_1\mathcal{B}_0\rangle & \langle\mathcal{A}_1\mathcal{B}_1\rangle & v_6 & v_3^* & v_4^* & \langle\mathcal{B}_0\rangle & \langle\mathcal{B}_1\rangle & v_7 \\
\langle\mathcal{B}_0\rangle & \langle\mathcal{A}_0\mathcal{B}_0\rangle & \langle\mathcal{A}_1\mathcal{B}_0\rangle & 1 & v_2 & v_3 & \langle\mathcal{A}_0\rangle & v_5 & \langle\mathcal{A}_1\rangle & v_7 & \langle\mathcal{B}_1\rangle \\
\langle\mathcal{B}_1\rangle & \langle\mathcal{A}_0\mathcal{B}_1\rangle & \langle\mathcal{A}_1\mathcal{B}_1\rangle & v_2^* & 1 & v_4 & v_5^* & \langle\mathcal{A}_0\rangle & v_7^* & \langle\mathcal{A}_1\rangle & v_8 \\
v_1^* & \langle\mathcal{A}_1\rangle & v_6^* & v_3^* & v_4^* & 1 & \langle\mathcal{A}_1\mathcal{B}_0\rangle & \langle\mathcal{A}_1\mathcal{B}_1\rangle & v_9 & v_{10} & v_{11} \\
\langle\mathcal{A}_0\mathcal{B}_0\rangle & \langle\mathcal{B}_0\rangle & v_3 & \langle\mathcal{A}_0\rangle & v_5 & \langle\mathcal{A}_1\mathcal{B}_0\rangle & 1 & v_2 & v_1 & v_{12} & \langle\mathcal{A}_0\mathcal{B}_1\rangle \\
\langle\mathcal{A}_0\mathcal{B}_1\rangle & \langle\mathcal{B}_1\rangle & v_4 & v_5^* & \langle\mathcal{A}_0\rangle & \langle\mathcal{A}_1\mathcal{B}_1\rangle & v_2^* & 1 & v_{13} & v_1 & v_{14} \\
\langle\mathcal{A}_1\mathcal{B}_0\rangle & v_3^* & \langle\mathcal{B}_0\rangle & \langle\mathcal{A}_1\rangle & v_7 & v_9^* & v_1^* & v_{13}^* & 1 & v_2 & \langle\mathcal{A}_1\mathcal{B}_1\rangle \\
\langle\mathcal{A}_1\mathcal{B}_1\rangle & v_4^* & \langle\mathcal{B}_1\rangle & v_7^* & \langle\mathcal{A}_1\rangle & v_{10}^* & v_{12}^* & v_1^* & v_2^* & 1 & v_{15} \\
v_2^* & v_5^* & v_7^* & \langle\mathcal{B}_1\rangle & v_8^* & v_{11}^* & \langle\mathcal{A}_0\mathcal{B}_1\rangle & v_{14}^* & \langle\mathcal{A}_1\mathcal{B}_1\rangle & v_{15}^* & 1
\end{pmatrix} \tag{3.6}$$

where we define the following unassigned variables

$$\begin{aligned}
v_1 &= \langle\mathcal{A}_0\mathcal{A}_1\rangle\,, & v_2 &= \langle\mathcal{B}_0\mathcal{B}_1\rangle\,, & v_3 &= \langle\mathcal{A}_0\mathcal{A}_1\mathcal{B}_0\rangle\,, \\
v_4 &= \langle\mathcal{A}_0\mathcal{A}_1\mathcal{B}_1\rangle\,, & v_5 &= \langle\mathcal{A}_0\mathcal{B}_0\mathcal{B}_1\rangle\,, & v_6 &= \langle\mathcal{A}_1\mathcal{A}_0\mathcal{A}_1\rangle\,, \\
v_7 &= \langle\mathcal{A}_1\mathcal{B}_0\mathcal{B}_1\rangle\,, & v_8 &= \langle\mathcal{B}_1\mathcal{B}_0\mathcal{B}_1\rangle\,, & v_9 &= \langle\mathcal{A}_1\mathcal{A}_0\mathcal{A}_1\mathcal{B}_0\rangle\,, \\
v_{10} &= \langle\mathcal{A}_1\mathcal{A}_0\mathcal{A}_1\mathcal{B}_1\rangle\,, & v_{11} &= \langle\mathcal{A}_1\mathcal{A}_0\mathcal{B}_0\mathcal{B}_1\rangle\,, & v_{12} &= \langle\mathcal{A}_0\mathcal{A}_1\mathcal{B}_0\mathcal{B}_1\rangle\,, \\
v_{13} &= \langle\mathcal{A}_0\mathcal{A}_1\mathcal{B}_1\mathcal{B}_0\rangle\,, & v_{14} &= \langle\mathcal{A}_0\mathcal{B}_1\mathcal{B}_0\mathcal{B}_1\rangle\,, & v_{15} &= \langle\mathcal{A}_1\mathcal{B}_1\mathcal{B}_0\mathcal{B}_1\rangle\,.
\end{aligned} \tag{3.7}$$

Now, if we further impose commutativity of all the measurements, namely $[\mathcal{A}_0, \mathcal{A}_1] = 0$, $[\mathcal{B}_0, \mathcal{B}_1] = 0$, the corresponding linear constraints reduce the number of variables. Explicitly, one gets $v_i^* = v_i$ for any $i = 1, \ldots, 15$, and also

$$\begin{aligned}
v_6 &= \langle\mathcal{A}_0\rangle\,, & v_8 &= \langle\mathcal{B}_0\rangle\,, & v_9 = v_{14} &= \langle\mathcal{A}_0\mathcal{B}_0\rangle\,, \\
v_{10} &= \langle\mathcal{A}_0\mathcal{B}_1\rangle\,, & v_{15} &= \langle\mathcal{A}_1\mathcal{B}_0\rangle\,, & v_{11} = v_{12} &= v_{13}\,.
\end{aligned} \tag{3.8}$$

For a visual representation, the variables that become identical because of the commutativity constraints are represented by the same color in (3.6). Let us notice that the above matrix can be seen as the equivalent of (2.16), expressed in terms of the four dichotomic random variables $\{\mathcal{A}_0, \mathcal{A}_1, \mathcal{B}_0, \mathcal{B}_1\}$.

For any set of observed correlations $\{\langle\mathcal{A}_x\rangle, \langle\mathcal{B}_y\rangle, \langle\mathcal{A}_x\mathcal{B}_y\rangle\}$, testing whether it is local can be done in the following steps: assigning the values to the

entries of Γ that can be derived from the observed correlations and leaving the remaining terms as variables, then checking whether there is an assignment for such variables such that the matrix is positive semidefinite.

For instance, it is possible to check that any set of correlations that violates the well-known CHSH inequality (2.56) is incompatible with a positive semidefinite matrix (3.6). We stress that a necessary condition to produce correlations that violate CHSH is that the measurements performed by each party does not commute with each other. This shows how the commutativity constraints imposed in the SDP test are crucial for the detection of the nonlocality of the observed correlations.

To conclude, we recall that, in this particular scenario, any set of nonlocal correlations has to violate the CHSH inequality, or symmetrical equivalent of it (cfr. Section 2.3.5). Therefore, it turns out that in this case the second level of the hierarchy is already capable of detecting any nonlocal correlation. That is, even if in this scenario the hierarchy is expected to converge at level $\nu' = 4$, the second level happens already to be tight to the local set.

3.2.4 Geometrical interpretation

Before presenting the applications of our method, we analyse it in a geometrical perspective, schematically represented in Figure 3.1. Recall that the set of local correlations $\mathcal{L}$ defines a polytope, i.e. a convex set with a finite number of extremal points. Such points coincide with the deterministic strategies $D(a_i|x_i, \lambda)$ introduced in (3.5) and can be easily defined for any multipartite scenario. As represented in Figure 3.1, the set of quantum correlations $\mathcal{Q}$ is strictly bigger than the local set. All the points lying outside the set $\mathcal{L}$ represent nonlocal correlations.

Determining whether some observed correlations are nonlocal corresponds to checking whether they are associated to a point outside the local set. A very simple way to detect nonlocality is by means of Bell inequalities. However, there can be nonlocal correlations that are not detected by a given inequality, meaning that they fall on the same side of the hyperplane as local correlations.

On the other hand, a very general technique to check if a point belongs to the local set consists in determining if it can be decomposed as a convex combination of its vertices [ZKBL99]. Such a question is a typical instance of a linear programming problem, for which there exist algorithms that run in a time that is polynomial in the number of variables (cfr. Section 2.1.1). Nevertheless, finding a convex decomposition in the multipartite scenario is generally an intractable problem because the number of deterministic strategies grows as d^{mN}. Already in the

simplest cases in which each party measures only $m = 2, 3$ dichotomic measurements, the best approach currently known stops at $N = 11$ and $N = 7$ respectively [GGH$^+$14].

Coming back to the SDP method presented in the previous section, we can now show how the technique can help in overcoming the limitations imposed on the linear program. Let us define the family of sets $\mathcal{L}_\nu$ as the ones composed by the correlations that are compatible with the moment matrix Γ defined by the observables $\mathcal{O}_\nu$ and the additional constraints of commuting measurements. Given that any local distribution has a quantum representation with commuting measurements, the series $\mathcal{L}_1 \supseteq \mathcal{L}_2 \supseteq \ldots \supseteq \mathcal{L}$ defines a hierarchy of sets approximating better and better the local set from outside. In Figure 3.1 we show a schematic representation of the first levels of approximations.

Interestingly, it can be seen that the first level of the hierarchy is not capable of detecting any nonlocal correlations. A simple way to understand it is that, in the moment matrix generated by $\mathcal{O}_1$, imposing commutativity of the local measurement does not result in any additional constraint in the entries. A clear example is given by the $N = 2$ case presented in the previous section. The moment matrix corresponding to the first level can be identified with the 5×5 top-left corner of (3.6). There, the only modification imposed by local commutativity is the condition for the matrix to be real, which can always be assumed when working with quantum correlations. Therefore, we can say that $\mathcal{L}_1 = \mathcal{Q}_1$, meaning that the first level of our relaxation coincides with the first level of the original NPA, thus resulting in an approximation of the quantum set from outside.

Since we are interested in focusing on the first non-trivial level that allows for nonlocality detection, we then consider $\mathcal{L}_2$. We notice that, at this level of the hierarchy, specifying the entries $\Gamma_{ij} = \mathrm{tr}(\mathcal{O}_i^\dagger \mathcal{O}_j \rho)$ requires knowledge of up-to-four-body correlators. Moreover, the amount of terms in the set $\mathcal{O}_2$ scales as the number of possible pairs of measurements $M_{x_i}^{a_i}$, that is, as $N^2 m^2 d^2$. This implies that the size of the moment matrix scales only quadratically with the number of parties and measurements, which is much more efficient compared to the exponential dependence d^{mN} of the linear program. Moreover, since the elements in the moment matrix involve at most four operators, this implies that the number of measurements to be estimated experimentally scales as $N^4 m^4 d^4$.

As mentioned before, checking whether a set of observed correlations belongs to $\mathcal{L}_2$ constitutes a SDP feasibility problem. Since we are addressing approximations of the local set, there will be nonlocal correlations that will fall inside $\mathcal{L}_2$ and that will not be distinguishable from the local correlations. Therefore, our technique can provide only neces-

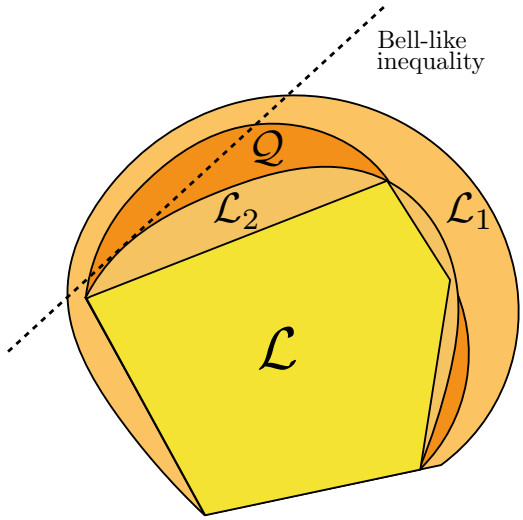

Figure 3.1: Pictorial representation of the sets of correlations, together with our approach to detection of multipartite nonlocality. The $\mathcal{L}$ and $\mathcal{Q}$ sets delimit the local and quantum correlations respectively. As discussed here, the first forms a polytope, namely a convex set delimited by a finite amount of extremal points, while the second, despite still being convex, is not a polytope. The light orange sets are the first representatives of the hierarchy $\mathcal{L}_1 \supseteq \mathcal{L}_2 \supseteq \ldots \supseteq \mathcal{L}$ approximating the local set from outside. It can be seen that some of the quantum correlations lie outside the $\mathcal{L}_2$, meaning that they are detected as nonlocal from the SDP relaxation at the second level. The dotted line shows a Bell-like inequality that can be obtained by the corresponding dual problem.

sary conditions for nonlocality. Nonetheless, we are able to find several examples in which this method is able to successfully detect nonlocal correlations arising from various relevant states, proving that it is not only scalable, but also a powerful method despite being a relaxation.

3.3 Applications

The goal of this section is to show that the presented SDP relaxation can be successfully employed for detection of the nonlocality arising from a broad range of quantum states. We focus particularly on exploring the efficient scaling of the method in terms of number of particles. To generate the SDP relaxations, we use the software Ncpol2sdpa [Wit15], and we solve the SDPs with Mosek [Mos].

We collect evidence that, from a computational point of view, the main limiting factor of the technique is not time but the amount of memory required to store the moment matrix. Indeed, the longest time that is taken to run one of the codes amounts to approximately 9 h [2]. Despite the memory limitation, the SDP technique allows us to consider multipartite scenarios that cannot be dealt with in the standard linear program approach to check locality. Indeed, for the scenarios with $m = 2, 3$, we are able to detect nonlocality for systems of up to $N = 29$ and $N = 15$ respectively, thus overcoming the current limits of [GGH+14].

In the following sections, we list the examples of states we consider. Given that we study cases with dichotomic measurements only, we present them in the expectation value form $\{M_{x_i}^{(i)}\}$.

3.3.1 W state

As a first case, we analyse the Dicke state with a single excitation, also known as the W state (2.31). Let us consider the simplest scenario of $m = 2$ dichotomic measurements per party, where each observer performs the same two measurements; that is, $M_0^{(i)} = X$ and $M_1^{(i)} = Z$ for all $i = 1, \ldots, N$. We are able to show that the obtained probability distribution is detected as nonlocal at level $\mathcal{L}_2$ for $N \leq 29$. We recall that in this scenario the complexity of this test scales as $O(N^4)$, in terms of both elements to assign in the moment matrix and measurements to implement experimentally.

We also study the robustness of our technique to white noise,

$$\rho_N(p) = (1-p)|W_N\rangle\langle W_N| + p\frac{\mathbb{1}_N}{2^N} \tag{3.9}$$

where $0 \leq p \leq 1$ and $\mathbb{1}_N$ represents the identity operator acting on the space of N qubits. We estimate numerically the maximal value of p, referred to as p_{max}, for which the given correlations are still nonlocal according to the SDP criterion. Figure 3.2 reports the resulting values as a function of the number of parties. While the robustness to noise decreases with the number of parties, the method tolerates realistic amounts of noise, always larger than 6%, for all the tested configurations.

Finally, in order to study the robustness of the proposed test with respect to the choice of measurements, we also consider a situation where the parties are not able to fully align their measurements and choose randomly two orthogonal measurements [WLB11]. More precisely, we assume that $M_0^{(i)} = \vec{x}_0^{(i)} \cdot \vec{\sigma}$ and $M_1^{(i)} = \vec{x}_1^{(i)} \cdot \vec{\sigma}$, where $\vec{\sigma} = (X, Y, Z)$ and

[2] The code used is available under an open source license at `https://github.com/FlavioBaccari/Hierarchy-for-nonlocality-detection`

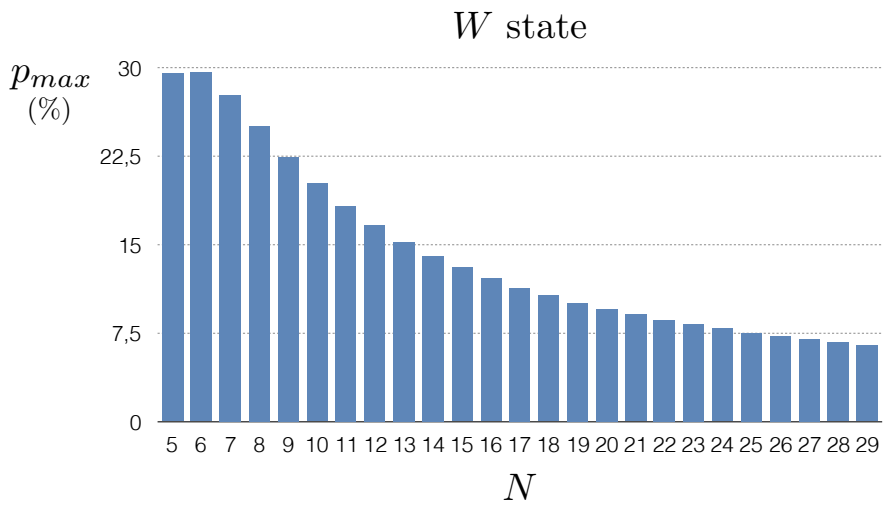

Figure 3.2: Robustness of nonlocality to white noise in the case of the W state, reported as a function of N.

$\vec{x}_0^{(i)}, \vec{x}_1^{(i)}$ are vectors chosen uniformly at random, with the only constraint of being orthogonal; namely $\vec{x}_0^{(i)} \cdot \vec{x}_1^{(i)} = 0$ for all $i = 1, \ldots, N$. We calculate numerically the probability p_{NL} for the corresponding correlations to be detected as nonlocal at the second level of the relaxation. To estimate p_{NL}, we compute the fraction N_{NL}/N_r of N_{NL} nonlocal distributions obtained over a total of $N_r = 1000$ rounds. The corresponding results are reported in the following table as a function of N.

N	p_{NL}	N	p_{NL}
3	50.2 %	7	21.0 %
4	44.4 %	8	12.8 %
5	38.4 %	9	6.3 %
6	28.8 %	10	2.7 %

The results for random measurements also exemplify one of the advantages of our approach with respect to previous entanglement detection schemes. Given some observed correlations, our test can be run and it sometimes detects whether the correlations are nonlocal and therefore come from an entangled state. To our understanding, reaching similar conclusions using entanglement witnesses or other entanglement criteria is much harder, as they require solving optimisation problems involving N-qubit mixed states.

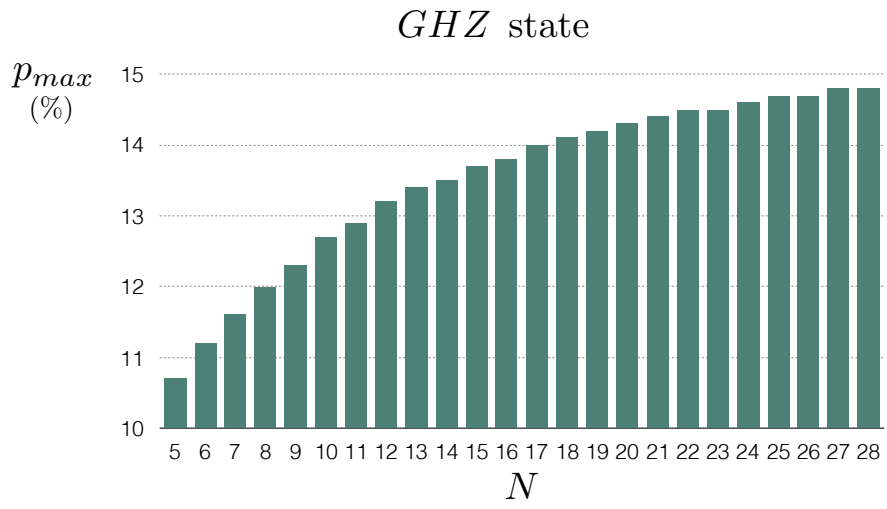

Figure 3.3: Robustness of nonlocality to white noise in the case of the GHZ state and 2 dichotomic measurements per party, reported as a function of N.

3.3.2 GHZ state

Another well-studied multipartite state is the GHZ state (2.30). Contrarily to the W state, such a state is not suited for detection of nonlocality with few-body correlations because all the k-body distributions arising from measurements on (2.30) are the same as those obtained by measuring the separable mixed state $\frac{1}{2}(|0\rangle\langle 0|^{\otimes k} + |1\rangle\langle 1|^{\otimes k})$. Therefore, in order to apply our nonlocality detection method to the GHZ state we need to involve at least one full-body term.

The solutions we present are inspired by the self-testing scheme for graph states introduced in [McK11]: the first scenario involves $m = 3$ dichotomic measurements per party; namely $M_0^{(i)} = X$, $M_1^{(i)} = D = \frac{1}{\sqrt{2}}(X+Z)$ and $M_2^{(i)} = Z$ for all $i = 1, \ldots, N$. To introduce full-body correlators in the SDP we define the set $\mathcal{O}_{mix} = \{\mathcal{O}_2, \langle M_0^{(1)} M_0^{(2)} \ldots M_0^{(N)}\rangle, \langle M_1^{(1)} M_0^{(2)} \ldots M_0^{(N)}\rangle\}$. The moment matrix corresponding to such set represents a mixed level of the relaxation, containing also two full-body correlators in the entries. However, since the number of added columns and rows is fixed to 2 for any N, this level is basically equivalent to level $\mathcal{L}_2$. Therefore, we preserve the efficient $O(N^4)$ scaling with the number of parties of elements in the moment matrix and measurements to implement.

By numerically solving the SDP associated to this mixed level of the

hierarchy we are able to confirm nonlocality of the correlations arising from the GHZ state and the given measurement for up to $N \leq 15$ parties. Moreover, we check that the number of full-body values that is necessary to assign is constant for any of the considered N, coinciding with the two correlators $\langle M_0^{(1)} M_0^{(2)} \ldots M_0^{(N)} \rangle$ and $\langle M_1^{(1)} M_0^{(2)} \ldots M_0^{(N)} \rangle$. Lastly, we estimate that the robustness to noise in this case does not depend on N and it amounts to $p_{max} \approx 0.17$.

As a second scenario, we also notice that one can produce nonlocal correlations from the GHZ at the level $\mathcal{O}_{mix}$ by considering $m = 2$ measurement choices only. Indeed, if ones considers $M_0^{(i)} = X$, $M_1^{(i)} = D$, the resulting correlations are detected as nonlocal for any $N \leq 28$ (the fact that we are not able to reach $N = 29$ is due to the mixed level of the relaxations, which results in a bigger matrix compared the scenario for the W state). Figure 3.3 shows the corresponding robustness to noise, computed in the same way as for the W state. For both configurations, the noise robustness of our scheme in detecting GHZ states seems to saturate for large N even if the computational (and experimental) effort scales polynomially.

3.3.3 Graph states

Graph states constitute another important family of multipartite entangled states (cfr. Section 2.2.4). Recall that GHZ state is also a graph state, associated to the so-called star graph. However, due to its particular relevance in quantum information theory, we prefer to treat its case in the previous section. Here we consider some other exemplary graph states such as the 1D and 2D cluster states and the loop graph state illustrated in Figure 3.4. Inspired by the self-testing scheme in [McK11], we consider that each party applies three measurements given by X, Z and D. We are able to detect nonlocality in the obtained correlations at level $\mathcal{L}_2$ for states involving up to $N = 15$ qubits. Again, the method at this level scales as N^4.

Interestingly, our approach for the detection of nonlocal correlations generated by graph states shows to be qualitatively different from McKague's scheme in [McK11]. While the latter requires correlators of an order that depends on the connectivity of the graph (namely, equal to 1 plus the maximal number of neighbours that each vertex has), our method seems - at least in some cases - to be independent of it. Indeed, we are able to detect nonlocality with four-body correlators in 2D cluster states, whose connectivity would imply five-body correlators for the self-testing scheme.

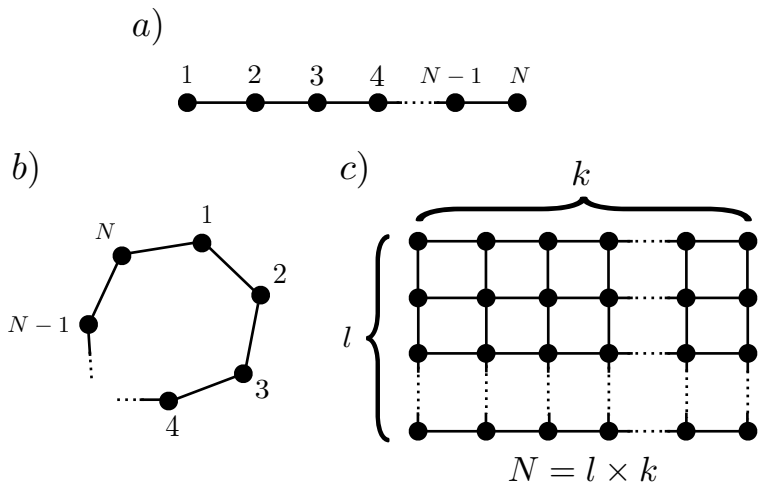

Figure 3.4: Representatives of the graphs associated to the classes of states that have been studied with the SDP method: a) Linear graph states. b) Loop graph states. c) 2D cluster states.

3.3.4 Explicit Bell inequalities

Another nice property of our nonlocality criterion comes from the fact that, as it can be put in a SDP form, it immediately provides a method to find experimentally friendly Bell inequalities involving a subset of all possible measurements. In fact, it turns out that the the SDP proposed in Sec. 3.2.1 has a dual formulation that can be interpreted as the optimisation of a linear function of the correlations that can be seen as a Bell-like functional, *i.e.* a functional that has a nontrivial bound for all correlations in $\mathcal{L}_k$ [NPA08] (see Appendix A.1 for details). Thus, if a set of correlations is found to be nonlocal, then the solution of the SDP provides a Bell inequality that is satisfied by correlations in $\mathcal{L}_\nu$ and that is violated by the tested correlations. Importantly, this Bell inequality can further be used to test other sets of correlations.

By using the two sets of correlations obtained by measuring 3 dichotomic observables per party in the GHZ state we are able to find the following Bell inequality:

$$\begin{aligned}\mathcal{I}^3_{mix} = &\sum_{i=2}^{N}\langle M_1^{(1)} M_2^{(i)}\rangle - \sum_{i=2}^{N}\langle M_0^{(1)} M_2^{(i)}\rangle + (N-1)\langle M_0^{(1)} M_0^{(2)} \ldots M_0^{(N)}\rangle \\ &+ (N-1)\langle M_1^{(1)} M_0^{(2)} \ldots M_0^{(N)}\rangle \leq 2(N-1) \end{aligned} \tag{3.10}$$

Numerically, we could certify the validity of this inequality for up to $N \leq 15$. Moreover, in principle the bound of $\beta_C = 2(N-1)$ is only guaranteed to be satisfied by correlations in $\mathcal{L}_{mix}$. However, motivated by the obtained numerical insight, we could prove that this bound actually coincides with the true local bound, and therefore, (3.10) is a valid Bell inequality for all N (for all the analytical proofs regarding this section, see Appendix A.1). This shows that, at least in this instance, the $\mathcal{L}_{mix}$ defined by the SDP relaxation associated to $\mathcal{O}_{mix}$ is tight to the local set.

It is also easy to show that (3.10) is violated by the GHZ state and the previously introduced choice of measurements. In particular, the value reached is $\mathcal{I}^3_{GHZ} = (1+\sqrt{2})(N-1)$ for any N. Given that both the local bound and the violation scale linearly with N, the robustness of nonlocality to white noise is constant and amounts to $p_{max} = \frac{\sqrt{2}-1}{\sqrt{2}+1} \approx 0.174$. We note that this results is in agreement with what is achieved numerically with the SDP for up to $N = 15$.

Similarly, we also find the following Bell inequality by using the set of correlations involving only two measurements per party described for the GHZ state:

$$\begin{aligned}\mathcal{I}^2_{mix} = &\sum_{i=2}^{N} \langle M_1^{(1)} M_1^{(i)} \rangle - \sum_{i=2}^{N} \langle M_0^{(1)} M_1^{(i)} \rangle + (N-1) \langle M_0^{(1)} M_0^{(2)} \ldots M_0^{(N)} \rangle \\ &+ (N-1) \langle M_1^{(1)} M_0^{(2)} \ldots M_0^{(N)} \rangle \leq 2(N-1) \end{aligned} \tag{3.11}$$

Once more, although this inequality is found numerically for up to $N \leq 28$ we prove that it is valid for any N. Moreover the bound $\beta_C = 2(N-1)$ is not only valid for correlation in $\mathcal{L}_{mix}$ but for any local set of correlations. The GHZ state and the given measurements result in a violation of $\mathcal{I}^2_{GHZ} = \frac{3+\sqrt{2}}{2}$. Given that in this case the relative violation is lower, we also have a lower robustness to noise, coinciding with $p_{max} = \frac{\sqrt{2}-1}{\sqrt{2}+3} \approx 0.09$ for any N. We notice that this value is different from the ones reported in Figure 3.3. The reason is that, to derive inequality (3.11) from the dual, we restrict to assigning only the values of the two-body correlations and the two full-body ones. On the other hand, the results in Figure 3.3 also take into account the assignment of the three- and four-body correlators, showing that this additional knowledge helps in improving the robustness to noise.

As a final remark, we stress that the measurement settings considered to derive an inequality from the dual might not be the optimal ones. For instance, we are able to identify different measurement choices for the case of (3.11) that lead to a higher violation of such an inequality,

hence resulting also in a better robustness to noise (see Appendix A.1 for details).

3.4 Discussion

In this Chapter we introduced a technique for efficient device-independent entanglement detection for multipartite quantum systems. It relies on a hierarchy of necessary conditions for nonlocality in the observed correlations. By focusing on the second level of the hierarchy, we consider a test that requires knowledge of up to four-body correlators only. We show that it can be successfully applied to detect entanglement of many physically relevant states, such as the W, the GHZ and the graph states. Besides being suitable for experimental implementation, our technique also has an efficient scaling in terms of computational requirements, given that the number of variables involved grows polynomially with N. This allows us to overcome the limitation of the currently known methods and to detect entanglement for states of up to few tens of particles. Moreover, the proposed technique has a completely general approach and it can be applied to any set of observed correlations. This makes it particularly relevant for the detection of new classes of multipartite entangled states.

We note that our techniques can also be used as a semidefinite constraints to impose locality. Consider, for instance, a linear function f of the observed correlations. One could find an upper bound on the value of this function over local correlations by maximising it under the constraint that the moment matrix Γ is positive semidefinite. A particular example could be to take f to be a Bell polynomial. Thus this approach would find a bound $f \leq \beta_C$ satisfied by all local correlations.

As a future question in this direction, it would be interesting to study how accurate is the approximation of the local set of correlations provided by the second level of the hierarchy. In some of the scenario that we consider the approximation is actually tight, but this is not generally the case. A possible approach could be to compare the local bound of some known Bell inequalities with that resulting from the hierarchy.

Furthermore, we notice that the second level of the hierarchy also has an efficient scaling with the number of measurements performed by the parties. This would allow us to inquire whether an increasing number of measurement choices can provide an advantage for entanglement detection in multipartite systems.

Lastly, we believe that the present techniques can be readily applied in current state-of-the-art experiments. For instance, experiments composed by up to 7 ions have demonstrated nonlocality using an exponentially

increasing number of full correlators [LZJ+14]. Moreover, recent experiments have produced GHZ-like states in systems composed by 14 ions [MSB+11] and 10 photons [WCL+16, CLY+17] with visibilities within the range required to observe a violation of the Bell inequalities presented here. We notice, however, that the measurements required to certify the presence of nonlocal correlations using our approach are different from the ones reported in these works.

Chapter 4

Detecting nonlocality depth in many-body systems

In this Chapter we address the question of quantifying the number of particles genuinely sharing nonlocal correlations in a multipartite system with the knowledge of two-body correlators only. More precisely, we adapt the techniques introduced in [TAS+14] to the problem of detection of nonlocality depth. These techniques are particularly relevant because they opened the way for the experimental detection of nonlocal correlations with trusted collective measurements in many-body systems such as Bose-Einstein condensates or thermal ensembles composed of thousands of particles [SBA+16, EKHK17].

We introduce a general framework allowing to derive Bell-like inequalities for nonlocality depth from symmetric two-body correlators. We characterize all such Bell-like inequalities for a finite number of parties and we show that they reveal Bell correlation depth $k \leq 6$ in arbitrarily large systems. We then show how Bell correlation depth can be estimated using quantities that are within reach in current experiments. On one hand, we use the standard multipartite Bell inequalities such the Mermin and Svetlichny ones to derive Bell correlations witnesses of any depth that involve only two collective measurements, one of which being the parity measurement. On the other hand, we show that our two-body Bell inequalities can be turned into witnesses of depth $k \leq 6$ that require measuring total spin components in certain directions. Interestingly, such a witness is violated by existing data from an ensemble of 480 atoms. The results of this Chapter are based on the original work published in [BTF+18].

4.1 Introduction

As argued in Section 2.3.1, local measurements on composite quantum systems may lead to nonlocal correlations that cannot be explained by any local realistic theory such as classical physics. More importantly, in recent years it has been understood that nonlocality is a powerful resource for device-independent applications that have no classical analogue, with the most prominent examples being device-independent quantum key distribution, device-independent entanglement detection, generation and amplification of randomness or self-testing.

However, to be able to fully exploit nonlocality as a resource, one first needs efficient methods to detect it in the composite quantum systems that can exhibit it. Since these systems can produce nonlocality upon measurement, i.e. statistics violating a Bell inequality, we say that their state is Bell correlated. Bell inequalities are naturally the most common tool of revealing both nonlocal statistics and Bell correlated states. Considerable amount of effort has been devoted to introduce various constructions of Bell inequalities. Still, the problem of nonlocality detection is much less advanced in the multipartite case than in the bipartite one. There are two main reasons for that: (i) the mathematical complexity of finding all Bell inequalities grows double exponentially with the number of parties, (ii) the experimental verification of nonlocality is much more demanding in the multipartite case, since individual settings assignment for each party is needed to test a Bell inequality. Moreover, most of the known multipartite Bell inequalities involve a large number of full-body correlation measurements and are thus difficult to estimate experimentally (see Ref. [WW01, ZB02]). Therefore, such inequalities are not suited to detect nonlocal correlations in many-body systems in which only a few collective measurements can be applied and one typically has access only to two-body correlations.

One of the ways to tackle these difficulties in the multipartite case is to consider Bell inequality involving only two-body correlators [TAS$^+$14]. This reduces the mathematical complexity of the problem and allows one to demonstrate that these inequalities are powerful enough to reveal nonlocality in composite quantum systems with an arbitrary number of particles [TAS$^+$15, TSV$^+$14, WSF$^+$17]. Moreover, these inequalities can be used to derive Bell correlation witnesses expressed in terms of just low order moments of a small number of collective spin measurements, which are routinely measured in certain many-body quantum systems (see Refs. [HSP10, ERIR$^+$08]). This makes these witnesses very practical and allowed for testing them in two experiments recently reporting on Bell correlations in many-body states consisting of 480 atoms [SBA$^+$16] in a

Bose-Einstein condensate and $5 \cdot 10^5$ particles [EKHK17] in a thermal ensemble.

However, the violation of these Bell inequalities and the corresponding witnesses only signals the presence of some kind of Bell correlations. In fact, it is unable to provide information regarding how many particles share genuine Bell correlations. This naturally raises the question of how to reveal the depth of non-locality in many-body systems. At first sight, the problem is challenging. Known Bell inequalities for genuine non-locality not only use expectation values involving all parties, they also require the ability to perform a different measurement on each party. Furthermore, the number of measurement settings scales exponentially with the number of parties.

The main aim of this Chapter is to address this question. We first introduce a general framework to study the problem of revealing the non-locality depth in multi-partite systems using two-body correlations only, hence guaranteeing that no high-order moment will be necessary at the level of the witness. The problem of detection of genuine nonlocality in this context is fully characterised for a relatively small number of parties, providing lists of Bell-like inequalities that do the job. Moreover, we give a Bell-like inequality detecting the nonlocality depth from 1 to 7 for any number of parties. We then turn to the question of witnessing Bell correlations depth in many-body systems. First, building on the Mermin and Svetlichny inequalities [Mer90, Sve87], we show that the nonlocality depth of any multipartite system can be tested via a Bell correlation witness, using only two trusted collective measurements. This gives access to genuine Bell correlations in many-body systems where one high-order measurement can be performed. Lastly, we derive witnesses corresponding to the two-body Bell inequalities we found and we apply them to detect the Bell correlations depth of a Bose-Einstein condensate with 480 atoms.

4.2 General framework and main results

The main objective of this Chapter is to provide efficient tools to assess the nonlocality depth of multipartite systems. In the following, we restrict the study to the $(N, 2, 2)$ Bell scenario, namely the case of N observers performing each two local measurements with dichotomic outputs (see Section 2.3.1 for more details). As we explained in Section 2.3.3, to study nonlocality depth in full generality one needs to characterise the polytopes of k-producible correlations, denoted $\mathcal{P}_{N,k}$, for any number of particles N and nonlocality depth k. However, to successfully address

this problem, one needs to overcome two major obstacles.

First, despite the general form of the vertices of $\mathcal{P}_{N,k}$ (cfr. Equation (2.47)), constructing them in practice requires previous knowledge about *all* the vertices of the no-signaling polytopes $\mathcal{NS}_p$ for $p \leq k$, whose determination is already a formidable task. Indeed, while the facets of the no-signaling polytopes are easy to enumerate for any number of particles, recall that its complete list of vertices has been derived only in the simplest scenarios of $N = 2, 3$ [PBS11]. It should also be mentioned that in [Fri12] a polyhedral duality between Bell inequalities and the vertices of the nonsignaling polytope in the $(N, 2, 2)$ scenario was established, thus proving that finding all vertices of $\mathcal{NS}_p$ is equivalent to find all tight Bell inequalities in $\mathcal{P}_p$. The difficulty in finding all Bell inequalities in a given scenario was already observed by Pitowsky in 1989 [Pit89], and it was later proven to be NP-hard even in a bipartite setting [BFL91].

Second, suppose one could actually list all the extremal points of $\mathcal{P}_{N,k}$. The size of this list would grow exponentially as a function of N: simply consider the L_k-partition consisting of the maximal amount of subsets of size k (plus a smaller subset if k does not divide N). Then, by denoting v_k the number of vertices of $\mathcal{NS}_k$, we see from (2.47) that the number of vertices of $\mathcal{P}_{N,k}$ will grow as $O(v_k^{\lfloor N/k \rfloor})$. This exponential growth with N already renders any effort to derive a complete list of Bell inequalities for nonlocality depth for large values of N futile.

To overcome these difficulties, we restrict our analysis to the scenario of symmetric two-body correlations, firstly introduced in [TAS+14]. That is, instead of working with the full probability distribution $p(a_1, \ldots, a_N|x_1, \ldots, x_N)$, we imagine that the only accessible information consists of the following one- and two-body expectation values

$$\langle M_x^{(i)} \rangle, \qquad \langle M_x^{(i)} M_y^{(j)} \rangle \tag{4.1}$$

with $i \neq j = 1, \ldots, N$ and $x, y = 0, 1$ (cfr. Equation (2.43)). Such an assumption is particularly relevant for experimental applications, since those quantities can be efficiently estimated with just a polynomial amount of measurements. In addition, this allows us to answer a fundamental question: whether two-body correlators; i.e., the minimal amount of information needed to detect nonlocality in a quantum system, are enough to reveal nonlocality depth in a multipartite system. Moreover, we look for Bell inequalities that are invariant under an exchange of any pair of parties, meaning that they are function of the symmetrised quantities

$$\mathcal{S}_x := \sum_{i=1}^{N} \langle M_x^{(i)} \rangle, \qquad \mathcal{S}_{xy} := \sum_{\substack{i,j=1 \\ i \neq j}}^{N} \langle M_x^{(i)} M_y^{(j)} \rangle \tag{4.2}$$

with $x, y = 0, 1$. Mathematically, this implies that instead of studying the full $\mathcal{P}_{N,k}$ polytope, we want to characterise its projection $\mathcal{P}^{2,S}_{N,k}$ onto the lower-dimensional space of symmetric one- and two-body correlators, spanned by the five quantities (4.2).

Therefore, we look for a complete characterisation of the symmetric two-body Bell inequalities that detect nonlocality depth, whose most general form is

$$I := \alpha\mathcal{S}_0 + \beta\mathcal{S}_1 + \frac{\gamma}{2}\mathcal{S}_{00} + \delta\mathcal{S}_{01} + \frac{\varepsilon}{2}\mathcal{S}_{11} + \beta_k \geq 0, \tag{4.3}$$

with

$$\beta_k = -\min_{\mathcal{P}^{2,S}_{N,k}} I, \tag{4.4}$$

where the minimum is taken over all correlations belonging to $\mathcal{P}^{2,S}_{N,k}$.

Recall that the case of $k = 1$ recovers the study of the local polytope, whose complete list of Bell inequalities is unknown already for $N \geq 4$. Interestingly, it turns out that restricting to its symmetric two-body projection dramatically simplifies the problem, as was extensively shown in [TAS$^+$14, TAS$^+$15]. More precisely, such a projection makes it possible to derive all the facets of the local polytope for scenarios with tens of particles, and also to obtain classes of inequalities valid for any N.

Here we take a step forward and look at the cases corresponding to $k > 1$. Remarkably, we see that many simplifications can be carried out in the generic nonlocality depth case as well. The rest of the Section is devoted to briefly summarise our results, as well as their applications to the study of correlations in many-body systems, while leaving the in-depth presentation to the Sections 4.2, 4.3.2 and 4.5.

Result 1. *The vertices of the polytopes $\mathcal{P}^{2,S}_{N,k}$ can be computed efficiently as functions of the vertices of the projected no-signaling polytopes $\mathcal{NS}^{2,S}_p$ of $p \leq k$ parties. For a fixed value of k, the number of vertices scales polynomially with N.*

Recall the first obstacle stated above, regarding the complexity of finding the vertices of $\mathcal{NS}_N$ for a general N. Our first result implies that, in order to study nonlocality depth with symmetric two-body correlators, it is not necessary to find all the vertices of $\mathcal{NS}_N$, and it is sufficient to find the vertices of its projection to the two-body symmetric subspace, $\mathcal{NS}^{2,S}_N$.

Note, however, that determining the projection of a polytope is not a simple task, especially if the original polytope is described in terms of inequalities, which is the case for $\mathcal{NS}_N$. The general procedure to

find such a projection relies on the Fourier-Motzkin elimination method (see Sec. 2.1.2), which has an exponential scaling with the number of components that need to be projected out (note that the number of correlators involving more than 2 parties already scales exponentially with N, therefore yielding an overall doubly-exponential scaling). Indeed, the $\mathcal{NS}_N$ polytope is parametrised by the correlators (2.43), and there are $3^N - 1$ of them, while $\mathcal{NS}_N^{2,S}$ is embedded in a five-dimensional space for any N (cfr. Eq. (4.3)); therefore, applying Fourier-Motzkin is basically impractical for any $N > 2$.

Nonetheless, in Section 4.2 we show that the structure of the no-signaling polytope can be exploited to dramatically reduce the complexity of the problem. In particular, we divide the projection operation into two steps: first, the symmetrisation one, which yields the polytope $\mathcal{NS}^S$, parametrised by the symmetric correlators (4.2) of any order; second, the projection onto the two-body space $\mathcal{NS}^{2,S}$, which consists in removing all the symmetric correlators of order higher than two. By following this procedure, we arrive at our second result, which is the technical key point of this work:

Result 2. *The facets of the $\mathcal{NS}_N^S$ polytopes can be efficiently obtained for any N. Then, the projection operation to get the desired $\mathcal{NS}_N^{2,S}$ polytopes involve projecting out a number of components that scales only as $\mathcal{O}(N^2)$.*

Combining the two results, we are able to make several advancements in the problem of detecting nonlocality depth in multipartite systems. Thanks to Result 2, we are able to obtain the complete list of vertices of the $\mathcal{NS}_N^{2,S}$ polytopes for up to $N = 6$ parties. This allows us to characterise the vertices of the polytopes of k-producible correlations of a nonlocality depth of $k \leq 6$. Because of the exponential reduction with respect to Result 1, it is then possible to obtain all the Bell inequalities detecting such nonlocality depths for systems of $N \leq 15$ particles. In Section 4.3.2 we present the main findings regarding those inequalities, among others the possibility of efficiently detecting GMNL up to 7 parties.

Moreover, we study a class of Bell inequalities, valid for any N, whose k-producible bound β_k varies with k and is violated by quantum correlations for sufficiently large N if $k \leq 6$. This leads to our third result, namely:

Result 3. *Nonlocality depth, for values of at least $k \leq 6$, can be detected with symmetric two-body correlators in systems composed of any number of particles.*

Up to now, all the results we have presented are purely device-independent. Therefore, if one were capable to perform a loophole-free Bell test among

the involved parties, one would be able to certify the aforementioned nonlocality depth of the correlations being produced. However, two-body permutationally invariant Bell inequalities have the extra feature that they can be indirectly measured via trusted collective observables and second moments thereof [TAS+14]. In Section 4.5 we turn our attention towards the application of our findings to the study of many-body systems. Importantly, in such scenario, the only information accessible is often represented by collective observables, which are enough to estimate the expectation values of (4.2).

Hence, at the price of introducing an additional assumption on the measurements performed, one can turn any Bell inequality into a correlation witness [SBA+16]. The violation of such witness can be interpreted as a detection of a state displaying Bell correlation depth k, i.e. an entangled state capable of producing k-nonlocal correlations.

Notice that thus far Bell correlations witnesses have been studied only in the context of two-body inequalities detecting standard nonlocal correlations. We first consider their application to already known full-body Bell inequalities capable of distinguishing nonlocality depth, such as the Mermin [Mer90] and Svetlichny inequalities [Sve87]. In Section 4.5.1 we show that, although being composed by an exponentially large number of terms, such inequalities can be related to witnesses involving only two collective measurements. The ability to detect the ultimate depth of nonlocal correlations, GMNL, from collective observables only, comes at the price that one of these collective observables, however, consists in a parity measurement, which becomes technologically demanding in large systems. This motivates us to turn our attention to the two-body Bell inequalities introduced here. In particular, we connect the class of Bell inequalities studied in Section 4.3.2 to witnesses related to the squeezing parameter in a many-body state and we show that

Result 4. *Entangled k-nonlocal states, for values of at least $k \leq 6$, can be detected in many-body systems of in principle any number of particles.*

To conclude, we apply this witness to already available experimental data from a Bose-Einstein condensate of few hundreds of atoms. We devote the rest of the Chapter to present our results in detail.

4.3 Characterising the sets of k-producible correlations with two-body correlators

Our aim in this section is the characterisation of the symmetric two-body polytopes of k-producible correlations $\mathcal{P}^{2,S}_{N,k}$. To this end, we also

determine the vertices of the projections of the no-signaling polytopes onto two-body symmetric correlations $\mathcal{NS}_N^{2,S}$ for small values of N.

4.3.1 Characterisation of the vertices of the k-producible two-body symmetric polytopes

Here we introduce a general description of all the vertices of the projected $\mathcal{P}_{N,k}^{2,S}$ polytopes. This description assumes previous knowledge of all the vertices of the symmetrised p-partite no-signaling polytope $\mathcal{NS}_p^{2,S}$ for each $p \leq k$.

Let us introduce the following notation. Let n_p be the number of vertices of $\mathcal{NS}_p^{2,S}$, with $1 \leq p \leq k$. We want to compute the values of that the correlators (4.2) take in the i-th vertex, with $1 \leq i \leq n_p$. Let $\vec{S}(p,i)$ denote the five-dimensional vector

$$\vec{S}(p,i) = (S_0(p,i), S_1(p,i), S_{00}(p,i), S_{01}(p,i), S_{11}(p,i)) \tag{4.5}$$

of one- and two-body symmetric expectation values for the i-th vertex of $\mathcal{NS}_p^{2,S}$. We denote by $\{\vec{S}(p,i)\}_{p,i}$ the list of all such five-dimensional vectors (4.5).

Each vertex of the two-body symmetric polytope of k-producible correlations $\mathcal{P}_{N,k}^{2,S}$, can be obtained as a projection of a vertex (2.47) onto the two-body symmetric subspace (cfr. Sec. 2.1.2). Interestingly, it can be parametrised by the populations $\xi_{p,i}$ with $p = 1, \ldots, k$ and $i = 1, \ldots, n_p$, representing the number of p-partite subgroups $\mathcal{A}_l$ in the k-partition of the set $\{A_1, \ldots, A_N\}$ (cfr. Sec. 2.3.3) that are adopting the same "strategy" from the list $\{\vec{S}(p,i)\}_{p,i}$. Indeed, since we are addressing permutationally invariant quantities, these are insensitive to the assignment of a strategy to a specific group of parties, hence the only relevant information is about the number of parties adopting each given set of correlations [TAS$^+$14, TAS$^+$15].

Recall that parties are divided into subsets of size at most k, and each subset of size p chooses one out of n_p strategies. Therefore, the populations $\xi_{p,i}$, weighted by p, form a partition of N, that is, $\xi_{p,i}$ are integer numbers satisfying the conditions $\xi_{p,i} \geq 0$ and

$$\sum_{p=1}^{k} \sum_{i=1}^{n_p} p\, \xi_{p,i} = N. \tag{4.6}$$

By running over all populations $\xi_{p,i}$ obeying (4.6), one spans the whole set of vertices of the polytope $\mathcal{P}_{N,k}^{2,S}$. Moreover, denoting by $\vec{\xi}$ the vector with components $\xi_{p,i}$, the symmetrised one- and two-body expectation

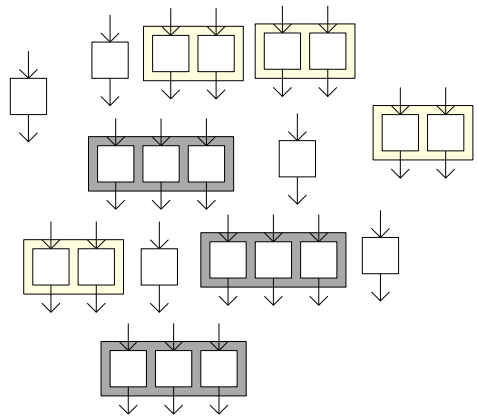

Figure 4.1: A possible L_k-partition corresponding to a vertex of $\mathcal{P}^{2,S}_{N,k}$, for $N = 22$, $k = 3$ and $L = 12$. Here we have taken a 12_3-partition consisting of 5 subsets of size 1, 4 subsets of size 2 and 3 subsets of size 3. Each of the 5 parties that are alone can choose one out of the $n_1 = 4$ possible local deterministic strategies. Counting how many particles choose the i-th strategy, where $1 \leq i \leq n_1$, determines $\xi_{1,i}$. Each pair of particles highlighted in yellow can choose one out of the n_2 possible vertices of $\mathcal{NS}_2$ and each triplet of particles highlighted in gray can choose one out of the n_3 PR-boxes highlighted in gray. The remaining coordinates of $\vec{\xi}$ are obtained analogously by counting. See Appendix B.1 for a detailed explanation on how to obtain the values (4.7) and (4.8) from $\vec{\xi}$.

values for the vertices of $\mathcal{P}^{2,S}_{N,k}$ can be expressed as

$$S_x(\vec{\xi}) = \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i} S_x(p,i) \tag{4.7}$$

and

$$\begin{aligned} S_{xy}(\vec{\xi}) \;=\; & \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i} S_{xy}(p,i) + \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i}(\xi_{p,i}-1) S_x(p,i) S_y(p,i) \\ & + \sum_{\{p,i\} \neq \{q,j\}} \xi_{p,i} \xi_{q,j} S_x(p,i) S_y(q,j), \end{aligned} \tag{4.8}$$

where we used the fact that $\langle M_x^{(i)} M_y^{(j)} \rangle = \langle M_x^{(i)} \rangle \langle M_y^{(j)} \rangle$ whenever the parties i and j belong to different groups, and $\{p,i\} \neq \{q,j\}$ means that $p \neq q$ or $i \neq j$ (cfr. Appendix B.1 for the details of the calculation and Fig. 4.1 for a pictorial representation).

Hence, from (4.7) and (4.8) we can see that all the vertices of the $\mathcal{P}^{2,S}_{N,k}$ can be directly computed as a function of the vertices of the projected no-signaling polytopes. In particular, we now prove that since their number is entirely encoded in the population vector $\vec{\xi}$, it grows only as $O(N^k)$.

Let $k \leq N$ be a constant, n_p be the number of vertices of $\mathcal{NS}^{2,S}_p$, and $n' = \max_p n_p$. Let us then define

$$\lambda_p = p \sum_{i=1,\ldots,n_p} \xi_{p,i}. \tag{4.9}$$

and group the components of λ_p into a vector $\vec{\lambda}$. Observe that $\vec{\lambda}$ forms a partition of N in k elements, where the p-th element is a multiple of p. Let us denote this fact as $\vec{\lambda} \vdash'_k N$. For a given p between 1 and k, we have to choose how many ways there are to partition λ_p/p into n_p possibly empty subsets. This is given by

$$\binom{\lambda_p/p + n_p - 1}{n_p - 1} \tag{4.10}$$

ways. Therefore, the total number of partitions satisfying (4.6) is given by

$$\sum_{\vec{\lambda} \vdash'_k N} \prod_{p=1}^{k} \binom{\lambda_p/p + n_p - 1}{n_p - 1}. \tag{4.11}$$

Now we are going to give an upper bound to (4.11) just to show a polynomial scaling in k. Since $\lambda_p/p \leq N$ and $n_p \leq n'$, we have the bound

$$\begin{aligned} \sum_{\vec{\lambda} \vdash'_k N} \prod_{p=1}^{k} \binom{\lambda_p/p + n_p - 1}{n_p - 1} &\leq \sum_{\vec{\lambda} \vdash'_k N} \binom{N + n' - 1}{n' - 1}^k \\ &\leq \binom{N + k - 1}{k - 1} \binom{N + n' - 1}{n' - 1}^k = O(N^{\zeta n' k}), \end{aligned} \tag{4.12}$$

where $\zeta > 1$ is some constant. Note that $\binom{N+k-1}{k-1}$ counts the number of partitions of N into k possibly empty subsets, which is clearly greater than the number of partitions of N into k possibly empty subsets satisfying the extra condition of λ_p being divisible by p. Since n' is constant because k is constant, the overall scaling is polynomial in N.

Therefore, given that the expressions (4.7) and (4.8) allow us to compute efficiently the vertices of the $\mathcal{P}^{2,S}_{N,k}$, the only remaining difficulty is to obtain the lists $\{\vec{S}(p,i)\}_{p,i}$ of vertices of the projected no-signaling polytopes, which we address in Section 4.3.2.

4.3.2 Projecting the nonsignaling polytopes

In order to generate the vertices of the symmetric two-body polytope of k-producible correlations $\mathcal{P}^{2,S}_{N,k}$, we need to know the vertices of the nonsignaling polytope $\mathcal{NS}_p$ in the two-body symmetric space for $2 \leq p \leq k$ parties. To this aim, we need to determine its projection $\mathcal{NS}^{2,S}_p$ onto the two-body symmetric space spanned by (4.2) for any $p = 2, \ldots, k$.

As already mentioned, the vertices of $\mathcal{NS}_p$ for $p > 3$ are unknown and difficult to determine. On the contrary, its facets are easy to describe by the positivity constraints, which in the correlators picture can be stated as (cfr. Eq. (2.40) and (2.44)):

$$\sum_{k=1}^{p} \sum_{1 \leq i_1 < \ldots < i_k \leq p} (-1)^{\sum_{l=1}^{k} a_{i_l}} \left\langle M^{(i_1)}_{x_{i_1}} \ldots M^{(i_k)}_{x_{i_k}} \right\rangle + 1 \geq 0, \tag{4.13}$$

for all the possible outcomes $a_{i_1}, \ldots, a_{i_N} = 0, 1$ and measurement choices $x_1, \ldots, x_N = 0, 1$.

Recall that the default approach to find the projections $\mathcal{NS}^{2,S}_p$ onto the two-body symmetric space, namely the Fourier-Motzkin procedure (see Section 2.1.2), becomes impractical already for $p = 3$, due to exponential number of components to project out. Nevertheless, in what follows we show how to overcome this difficulty by making use of the properties of the $\mathcal{NS}_p$ set with respect to the projection we are interested to perform.

To this end, let us denote by V_2 the subspace spanned by one- and two-body expectation values (4.1) and by V_{sym} the subspace spanned by the symmetrised correlators of any order:

$$S_{x_1 \ldots x_l} = \sum_{i_1 \neq \ldots \neq i_l = 1}^{p} \left\langle M^{(i_1)}_{x_1} \ldots M^{(i_l)}_{x_l} \right\rangle \tag{4.14}$$

with $x_i = 0, 1$ and $l = 1, \ldots, p$. We then define π_2, π_{sym} as the linear projections onto the V_2 and V_{sym} respectively; that is, π_2 discards all correlators that involve more than 2 parties and π_{sym} sums all the permutations of the correlators of a given order. We will use the fact that, in this notation, the projection we want to compute can be divided into two intermediate steps as $P = \pi_2 \circ \pi_{\text{sym}} = \pi_{\text{sym}} \circ \pi_2$, where the order in which the projections π_2 and π_{sym} are applied to $\mathcal{NS}_p$ does not change the result. In other words, the following diagram is commutative:

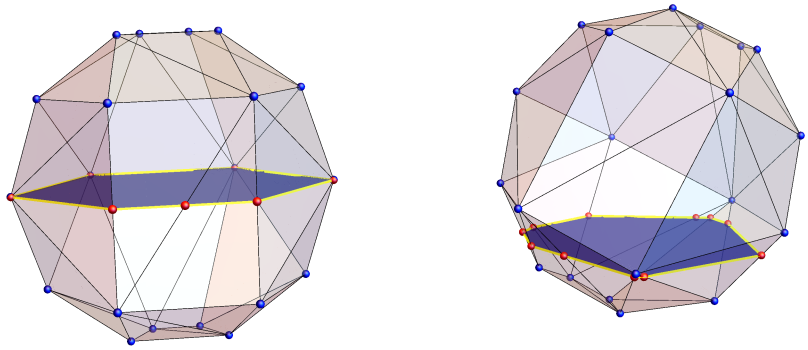

Figure 4.2: A cartoon picture illustrating the cases when projection and intersection of a polytope with a hyperplane are the same operation (left) and the generic case in which the intersection of a polytope with a hyperplane is strictly contained into its projection onto the same hyperplane (right).

$$\begin{array}{ccc} \mathcal{NS}_p & \xrightarrow{\pi_2} & \mathcal{NS}_p^2 \\ \downarrow{\scriptstyle \pi_{\text{sym}}} & & \downarrow{\scriptstyle \pi_{\text{sym}}} \\ \mathcal{NS}_p^S & \xrightarrow{\pi_2} & \mathcal{NS}_p^{2,S} \end{array}$$

This property follows from the fact that each coordinate of $\mathcal{NS}_p$ participates solely in one coordinate of $\mathcal{NS}_p^{2,S}$ (cfr. Eq. (4.2)).

We therefore choose to perform the projection as $P = \pi_2 \circ \pi_{\text{sym}}$, hence first computing the symmetrised polytope $\mathcal{NS}_p^S$ and then projecting it onto the two-body space. At this stage is then crucial noting that the no-signaling set is invariant under parties permutation. We now prove that this implies a very useful result, namely that the projection of this set onto V_{sym} coincides with the intersection between $\mathcal{NS}_p$ and V_{sym}, an idea which we illustrate in Fig. 4.2, i.e.

$$\text{int}_{\text{sym}}(\mathcal{NS}_p) = \pi_{\text{sym}}(\mathcal{NS}_p). \tag{4.15}$$

Let us first recall what we mean by the intersection. To do so, consider

the coordinates

$$T^{j_1\dots j_l}_{x_1\dots x_l} = \left(\sum_{i_1\neq\dots\neq i_l=1}^{p}\right)\langle M^{(j_1)}_{x_1}\dots M^{(j_l)}_{x_l}\rangle - S_{x_1\dots x_l}. \tag{4.16}$$

Taken together with the symmetrised S, these correlators provide an over-complete parametrisation of the no-signaling probability space: any correlator $\langle M^{(j_1)}_{x_1}\dots M^{(j_l)}_{x_l}\rangle$ can be recovered from the corresponding T and S variables. Moreover, these coordinates conveniently identify the subspaces that we are interested in: the symmetric subspace is spanned by the S variables, while its orthogonal complement by the T variables. In other words, all correlations in the symmetric subspace have all T components equal to zero (however, the variables themselves before projection need not to be zero). Moreover, the one- and two-body space has all S and T parameters equal to 0 for $l > 2$.

Using the above notation, we define $\mathrm{int}_{\mathrm{sym}}(\mathcal{NS}_p)$ as the set that contains all no-signaling correlations for which all the variables $T^{j_1\dots j_l}_{x_1\dots x_l} = 0$ (cfr. Section 2.1.2 for a more formal introduction to projection and intersection). Now, if a vertex v of $\mathcal{NS}_p$ (which may have both non-zero S and T components) leads to an extremal vertex after projection onto V_{sym}, then all images $v_\alpha = \tau_\alpha(v)$ of v under the party permutations $\{\tau_\alpha\}_\alpha$ are also in $\mathcal{NS}_p$, and lead to the same point in V_{sym} after projection. This follows directly from the invariance of $\mathcal{NS}_p$ under party permutations. Then, the convex combination of these points $\overline{v} \propto \sum_\alpha v_\alpha$ also gives rise to the same extremal point in V_{sym}. However, a direct computation shows that the point $\overline{v}$ already belongs to the symmetric subspace, because all of its T variables are zero. Hence, all extremal points of the projection of $\mathcal{NS}_p$ onto the symmetric subspace belong to the intersection of the no-signaling polytope with the symmetric subspace, and we can replace the projection operation π_{sym} by the intersection.

The main advantage of this approach is that the facets of the intersection of a polytope can be efficiently computed from the facets of the original one. Therefore, we only need to apply the Fourier-Motzkin method to perform the projection of $\mathcal{NS}^S_p$ onto the two-body space V_2. In this case the number of variables to discard does not grow exponentially with N. Indeed, the number of symmetric correlators $S_{x_1\dots x_l}$ with $x_j = 0, 1$ and $l = 1, \dots, p$ scales as $(1/2)(p+1)(p+2) - 1$ and, since one has to discard all the terms with $l > 2$, we need to eliminate only $(1/2)(p+1)(p+2) - 6 \approx \mathcal{O}(p^2)$ terms.

This simplification allows us to obtain the complete list of vertices of the $\mathcal{NS}^{2,S}_N$ polytopes for $N \leq 6$ particles, thus improving significantly over the already known results. For the $N = 2, 3, 4$ cases the lists of

vertices are presented in Tables B.2–B.4 in Appendix B.1, whereas in the case $N = 5, 6$ the list contains more than a hundred vertices and therefore we could not present it here. In the next section we implement these findings to construct Bell-like inequalities detecting k-nonlocality in multipartite correlations.

4.4 Bell-like inequalities for nonlocality depth from two-body correlations

We are now ready to demonstrate that two-body Bell-like inequalities are capable of witnessing nonlocality depth in multipartite correlations. First of all, we remind that, by following the procedure given in Section 4.3.1, we are able to construct the list of vertices of the k-nonlocal two-body symmetric polytopes for any number of parties N and producibility $k \leq 6$. By solving the convex hull problem, such lists allow us to derive the corresponding complete set of facets of the k-nonlocal polytopes (cfr. Section 2.1.1). To do so, we use the dual description method software CDD [Fuk97], and, thanks to both the low dimension of the space and the polynomial scaling of the k-producible vertices, we are able to do that for scenarios involving up to $N = 15$ parties.

In particular, since these inequalities can test against k-producibility with $k \leq 6$, we can identify all the symmetric two-body inequalities that detect genuine multipartite nonlocality (GMNL) for systems of $N \leq 7$ particles (see Appendix B.5 for the complete lists). Interestingly, we find that no inequality of such kind can be violated by quantum mechanics in the tripartite case. That is, symmetric two-body correlations provide not enough information to detect GMNL in three-partite quantum states. This is no longer the case for four parties; indeed, the following facet

$$\mathcal{I}^4_{GMNL} := -12S_0 + 9S_1 + 3S_{00} - 6S_{01} + \frac{1}{2}S_{11} + 42 \geq 0 \qquad (4.17)$$

detects GMNL and is violated by quantum mechanics with a ratio $(\beta_Q - \beta_3)/\beta_3$ of at least 1.3%, where β_Q is the maximal quantum value of the corresponding Bell expression.

Interestingly, our lists of inequalities sometimes contain also the Bell expressions introduced already in [TAS$^+$14, TAS$^+$15], thus showing that such classes are actually capable of detecting a nonlocality depth higher than two. In particular, we can find inequalities that test against any k-producibility for $k \leq 5$ that belong to the class (91) introduced in Ref. [TAS$^+$15]. This class is particularly interesting since it was shown to be violated by Dicke states. Moreover, among the facets of the GMNL

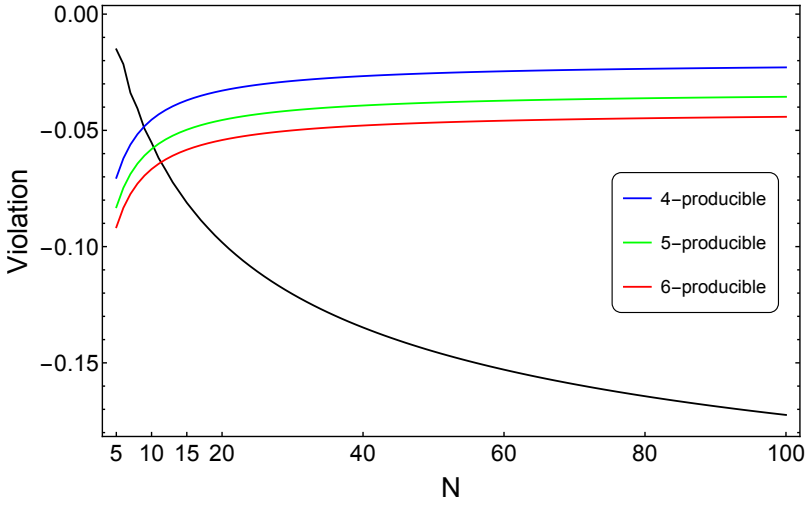

Figure 4.3: Plot of the quantum violation $(\beta_Q - \beta_1)/2N$ (black line) of the inequality (4.19) obtainable by following the procedure in [TAS+15]. The violation is compared with the - appropriately rescaled - k-producible bounds $(\beta_k - \beta_1)/2N$ for the same inequality (coloured lines) for values $k = 4, 5, 6$. Recall that the bounds for $k \leq 3$ coincide with the local one, hence they are not shown in the plot.

polytope for $N = 5$, we find the following inequality

$$\mathcal{I}_W = 28S_0 + 28S_1 + 2S_{00} + 9S_{01} + 2S_{11} + 116 \geq 0, \tag{4.18}$$

which has a very similar structure to class (91) of Ref. [TAS+15]. Indeed, it can be shown that it is possible to violate such inequality with the five-partite Dicke state with one excitation, also known as the W state.

Lastly, we notice that the Bell expression (6) from Ref. [TAS+14], which for the sake of completeness we state here as,

$$\mathcal{I} := 2S_0 + \frac{1}{2}S_{00} + S_{01} + \frac{1}{2}S_{11} \tag{4.19}$$

appears in our lists sometimes as well, with a classical bound that clearly depends on degree of nonlocality depth that one is interested to detect. This is a particularly useful feature, since it implies that by the use of a single inequality one can infer the nonlocality depth by the amount of the quantum violation that is observed. Due to this property and also its relevance for experimental implementation (see Refs. [SBA+16, EKHK17]), we focus on this last inequality and determine its β_k for $k = 2, \ldots, 6$ and any number of parties (see Appendix B.1 for the details

of the calculations). In particular, we first obtain that for the simplest cases of $k = 2, 3$, the k-producible bound coincides with the local, i.e. $\beta_k = 2N$, meaning that the violation of such inequality actually detects already a nonlocality depth of at least 4. Then, for the higher values of k, we are able show that the bound takes the following simple form

$$\beta_k = 2N + \frac{1}{2} + \alpha_k N. \tag{4.20}$$

where the parameter α_k encodes the dependence on the nonlocality depth. More explicitly, we obtain $\alpha_4 = 2/49$, $\alpha_5 = 8/121$ and $\alpha_6 = 1/12$.

After having introduced k-producible bounds for inequality (4.19), it is important to show that they can be used in practice to witness the nonlocality depth that could be displayed by quantum states. First of all, we have to show that the different bounds β_k can be violated by correlations obtained by properly choosing a quantum state and some local measurements. This can be done in a scalable way by following the procedure in [TAS+14] and constructing the permutationally invariant Bell operator corresponding to the expression (4.19). Notice that to do so we assume for simplicity that each party performs the same measurements

$$M_0^{(i)} = \cos(\theta) Z_i + \sin(\theta) X_i, \qquad M_1^{(i)} = \cos(\phi) Z_i + \sin(\phi) X_i, \tag{4.21}$$

where $\theta, \phi \in [0, 2\pi)$, and X and Z are the standard Pauli matrices. Then, by computing the minimal eigenvalue of the resulting Bell operator $\mathcal{B}(\theta, \phi)$ and optimizing over the choice of angles, one obtains the maximal quantum violation of (4.19) attainable with same measurements settings on each site. By performing these numerical checks, whose results are compared in Figure 4.3, it is possible to show that the bound β_k for $k \leq 3$ starts being violated for $N = 5$ parties, while for the higher cases $k = 4, 5$ the violation appears from $N = 9$ and $N = 11$ respectively. Moreover, if we take into account the analytical class of states introduced in Ref. [TAS+15] (cfr. Section 5.2), we can show that for a high enough number of parties it violates all the bounds that we have just derived. Indeed, let us recall that this class of states can achieve a relative violation $(\beta_Q - \beta_1)/\beta_1$ of (4.19) that tends to $-1/4$ when $N \to \infty$. By using this result, it is easy to show that β_Q exceeds β_k for any $k \leq 6$, at least in the asymptotic limit, confirming the numerical evidence shown in Figure 4.3. To conclude, in the following Section we also present how to apply

our results to an experimental setting.

4.5 Experimental witnessing of k-body Bell correlations

The inequalities introduced in the previous sections provide efficient tools to study the nonlocality depth of correlations produced by multipartite states. In fact, being based on two-body correlations only, they require at most performing $\mathcal{O}(N^2)$ measurements. This makes these inequalities particularly amenable for currently available photonic and atomic systems composed of few tens of particles [WLH$^+$18a, SXL$^+$17, FMM$^+$18].

Moreover, as already noticed in [TAS$^+$14, SBA$^+$16], the symmetrised one- and two-body correlators (4.2) can be estimated by means of collective measurements. Recall, however, that this connection can be established only if one makes the additional assumption that the measurements performed locally correspond indeed to spin projections along some direction. Although not providing a fully device-independent test, inequalities of the form (4.3) can still be turned into witnesses that quantify the amount of Bell correlations exhibited by a many-body system. More precisely, violating such witnesses has to be interpreted as a detection of *Bell correlations depth* in the state. In other words, they constitute Bell correlations witnesses for depth k that certify the presence of an entangled state that could display nonlocal correlations of depth $k+1$, if the single particles were brought far apart from each other and addressed separately.

In the following subsections, we study in more detail the available methods to quantify Bell correlations depth in a many-body state. First of all, we derive the witness corresponding to already known full-body inequalities capable of detecting nonlocality depth, such as the Mermin and Svetlichny Bell inequalities. Interestingly, we show that such a witness can actually be estimated by collective spin measurements along two directions only, although requiring a parity measurement that becomes too demanding for large systems. This shows how the two-body Bell inequalities introduced in this Chapter can provide a real advantage in terms of experimental feasibility. In order to exemplify such advantage, we derive the witness associated to inequality (4.19) and, by making use of already available data, show how it can be applied to detect Bell correlations depth in a BEC composed of hundreds of particles.

4.5.1 Witnessing genuine non-locality from Svetlichny and Mermin inequalities

The Mermin and Svetlichny Bell expressions are known to be suitable for the detection of non-locality depth in multipartite systems [BBGP09]. They thus suit very well our investigations. We here show the form of the corresponding witnesses for non-locality depth. Let us begin with the Svetlichny Bell expressions written in the following form [BBS+13]:

$$I_N^{\text{Svet}} = 2^{-N/2}\left[\sum_{\mathbf{x}|\mathbf{s}=0 \pmod 2} (-1)^{\mathbf{s}/2} E_{\mathbf{x}} + \sum_{\mathbf{x}|\mathbf{s}=1 \pmod 2} (-1)^{(\mathbf{s}-1)/2} E_{\mathbf{x}}\right], \tag{4.22}$$

where $\mathbf{s} = \sum_i x_i$ is the sum of all parties' settings (recall that $x_i \in \{0,1\}$), $\mathbf{x}|\mathbf{s} = i \pmod 2$ means that the summation is over those $\mathbf{x}$'s for which $\mathbf{s}$ is even for $i = 0$ or odd for $i = 1$, and, finally,

$$E_{\mathbf{x}} = \left\langle M_{x_1}^{(1)} \dots M_{x_N}^{(N)} \right\rangle \tag{4.23}$$

is a short-hand notation for an N-partite correlator. Using the same notation, we also introduce the Mermin Bell expression [Mer90], namely

$$I_N^{\text{Mermin}} = 2^{-(N-1)/2}\left[\sum_{\mathbf{x}|\mathbf{s}=0 \pmod 2} (-1)^{\mathbf{s}/2} E_{\mathbf{x}}\right], \tag{4.24}$$

For both the above inequalities, the k-producible bounds β_k can be explicitly computed and they can be used to reveal different nonlocality depth from observed correlations (cfr. Appendix B.3.3 for more details). In particular, the $(N-1)$-nonlocal bound is always smaller than the maximal quantum violation β_Q, meaning that these inequalities can detect genuine multipartite nonlocality for any number of particles. The drawback is that the sums in Eq. (4.22) and (4.24) involve 2^N terms in total. This makes the Svetlichny and Mermin inequalities very difficult to test in systems with a large number of parties. Nevertheless, in the following we show that if one is willing to assume that the measurements are well calibrated spin projections, then one can derive a witness that involves only collective measurement in two directions.

First of all, let us compute the Bell operators corresponding to (4.22) and (4.24) when one sets the measurement to be the ones leading to the maximal quantum violation. Interestingly, both inequalities lead to the same operator, namely

$$\mathcal{B}_N^{\text{Svetlichny}} = \mathcal{B}_N^{\text{Mermin}} = 2^{(N-1)/2}\left(|0\rangle\langle 1|^{\otimes N} + |1\rangle\langle 0|^{\otimes N}\right). \tag{4.25}$$

We can thus derive a common witness with which the nonlocality depth of any multipartite system can be evaluated. In particular, one can prove that the above operator can be bounded in the following way

$$\mathcal{B}_N^{\text{Svet}} \geq \sqrt{2}^{N-1} \left[X_1 \dots X_N + 4J_z^2 - N^2 \mathbb{1} \right] ,$$

where we have defined the collective spin operator $J_z = \sum_{i=1}^N Z_i$. Combining the k-nonlocal bounds of the Svetlichny and Mermin Bell expressions then allows us to write the following witness of Bell correlations depth:

$$\langle \mathcal{B}_N \rangle = \sqrt{2}^{N-1} \left\langle X_1 \dots X_N + 4J_z^2 - N^2 \mathbb{1} \right\rangle \leq 2^{(N - \lceil \frac{N}{k} \rceil)/2}. \tag{4.26}$$

Ineq. (4.26) shows that two settings are enough to conclude about the Bell correlation depth of a given state, that is, to test the capability of a state to violate a Svetlichny/Mermin bound for k-nonlocality. This provides a way to detect various depths of Bell correlations with just two measurement settings and no individual addressing of the parties. In particular, since the GHZ state (2.30) saturates all the inequalities we used in this section, the operator $\mathcal{B}_N$ is able to detect that GHZ states are genuinely Bell correlated.

Still, this scheme involves one parity measurement: the N-body term in the x direction. It is worth noticing that the evaluation of this term does not require an estimation of all the moment of the spin operator $J_x = \sum_i X_i$ in the x direction (which would require a gigantic amount of statistics to be evaluated properly whenever $N \gg 1$). Rather, this term corresponds to the parity of the spin operator J_x, i.e. a binary quantity, and can thus be evaluated efficiently. However, an extreme resolution is required to estimate this quantity; failure to distinguish between two successive values of J_x can entirely randomise its parity.

The next section aims at detecting the nonlocality depth of multipartite states with two-body correlators only.

4.5.2 Witnessing with two-body correlations only

In the same spirit as [TAS+14, SBA+16, WSF+17], we derive a witness for Bell correlations of depth k from the expression $\mathcal{I} + \beta_k \geq 0$, where $\mathcal{I}$ is defined in Eq. (4.19). We assume that $M_0^{(i)}$ and $M_1^{(i)}$ are spin projection measurements on the ith party, along directions $\mathbf{n}$ and $\mathbf{m}$, respectively. This allows us to write $M_0^{(i)} = \boldsymbol{\sigma}^{(i)} \cdot \mathbf{n}$ and $M_1^{(i)} = \boldsymbol{\sigma}^{(i)} \cdot \mathbf{m}$, where $\boldsymbol{\sigma}^{(i)}$ is the vector of Pauli matrices acting on the ith party, and to express all correlators appearing in the Bell inequality as measurements of the collective spin operator $J_{\mathbf{n}} = (1/2) \sum_{i=1}^N \boldsymbol{\sigma}^{(i)} \cdot \mathbf{n}$. With the substitution

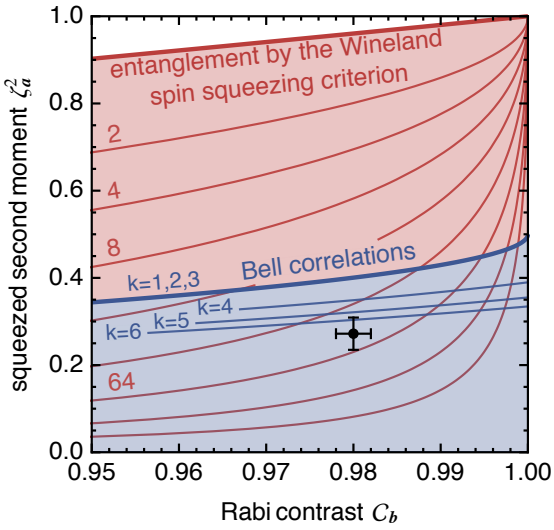

Figure 4.4: **Quantification of the Bell correlation depth in a BEC with inequality (4.28) and connection to spin squeezing and entanglement.** Black: the data reported in Ref. [SBA+16] expressed in terms of the Rabi contrast $\mathcal{C}_{\mathbf{b}}$ and the squeezed second moment $\zeta^2_{\mathbf{a}}$, with 1σ error bars. The number of particles is $N = 480$. Blue shaded region: Bell correlations detected by violation of inequality (4.28) for $k = 1$. Red shaded region: entanglement witnessed by spin squeezing [WBIH94, SDCZ01]. Red lines: limits on $\zeta^2_{\mathbf{a}}$ below which there is at least $(k+1)$-particle entanglement [SM01], increasing in powers of two up to $k = 256$. Blue lines: limits on $\zeta^2_{\mathbf{a}}$ below which there are Bell correlations of depth at least $k+1$, for $k = 1, \ldots, 6$.

$\mathbf{m} = 2(\mathbf{a}\cdot\mathbf{n})\mathbf{a} - \mathbf{n}$ we arrive at the inequality (see Ref. [SBA+16] for details).

$$-\left|\left\langle \frac{J_{\mathbf{n}}}{N/2}\right\rangle\right| + (\mathbf{a}\cdot\mathbf{n})^2\left\langle \frac{J^2_{\mathbf{a}}}{N/4}\right\rangle - (\mathbf{a}\cdot\mathbf{n})^2 + \frac{\beta_k}{2N} \geq 0, \tag{4.27}$$

which is satisfied by all states with Bell correlations of depth at most k. In other words, the violation of Ineq. (4.27) witnesses that the state of the system contains Bell correlations of depth (at least) $(k+1)$.

It is now convenient to define the spin contrast $\mathcal{C}_{\mathbf{n}} = \langle 2J_{\mathbf{n}}/N\rangle$ and the scaled second moment $\zeta^2_{\mathbf{a}} = \langle 4J^2_{\mathbf{a}}/N\rangle$. Furthermore, we express $\mathbf{n} = \mathbf{a}\cos(\theta) + \mathbf{b}\sin(\theta)\cos(\phi) + \mathbf{c}\sin(\theta)\sin(\phi)$, with the ortho-normal vectors $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c} = \mathbf{a}\times\mathbf{b}$ with $\times$ denoting the vector product. With these

definitions, one can obtain the witness [SBA+16]

$$\zeta_{\mathbf{a}}^2 \geq \frac{2 - \beta_k/(2N) - \sqrt{[\beta_k/(2N)]^2 - \mathcal{C}_{\mathbf{b}}^2}}{2}, \tag{4.28}$$

which involves the measurements of $\zeta_{\mathbf{a}}$ and $\mathcal{C}_{\mathbf{b}}$, for the two orthogonal directions $\mathbf{a}$ and $\mathbf{b}$. The violation of Ineq. (4.28), for a given β_k, witnesses that the state contains Bell correlations with a depth of (at least) $k+1$.

An interesting comparison is made with the Wineland spin-squeezing criterion
[WBIH94], according to which entanglement is present if $\zeta_{\mathbf{a}}^2 < \mathcal{C}_{\mathbf{b}}^2$ [SBA+16]. This criterion was also shown to be able to quantify the degree of entanglement in the state [SM01], $(k+1)$-particle entanglement is witnessed by measuring values of $\zeta_{\mathbf{a}}^2$ below some threshold, see Fig. 4.4 (red lines). In Fig. 4.4 we plot the bounds given by Eq. (4.28), for $k = 1, \ldots, 6$, together with the entanglement bound obtained from the Wineland criterion [SM01], and the experimental point measured in Ref. [SBA+16]. A statistical analysis on the probability distribution estimated experimentally [SBA+16] gives likelihoods of 99.9%, 97.5%, 90.3% and 80.8% for 1/2/3-, 4-, 5- and 6-body nonlocality respectively. This likelihood can be interpreted as, for example, a p-value of $1 - 80.8\% = 19.2\%$ for rejecting the hypothesis: *The experimental data were generated by a state that has no 6-body nonlocality, in the presence of Gaussian noise.*

4.6 Discussion

In this Chapter we studied the problem of finding efficient ways to detect the nonlocality depth of quantum correlations. Nonlocality depth is a relevant concept in the study of multipartite systems, because it contains the information of how many particles share genuine Bell correlations in their state. In analogy to the case of nonlocality, detecting nonlocality depth is a computationally very demanding problem.

We first exploit the framework of two-body symmetric correlations introduced in [TAS+14], to provide means of certifying nonlocality depth in many-body physics that meet the requirements of current experiments. By developing a general framework to describe the set of correlations of a given nonlocality depth, we are able to show that two-body symmetric correlations are enough to distinguish such depth. We do so by completely characterising the set of Bell inequalities that detect $k-$nonlocality with respect to no-signaling resources for values of $k \leq 6$ and a fixed number of particle $N \leq 15$. Remarkably, we also show that detecting nonlocality

depth can be done efficiently for any fixed k, that is, involving a polynomial amount of computational resources. Moreover, we take an explicit example of inequality and show that it can be used to witness the depth of Bell correlations for any number of parties.

Lastly, we comment on the practical application of our techniques to large many-body states. As a initial comparison, we turn to the known Bell inequalities such as the Mermin or Svetlichny one, that allow for detection of nonlocality depth in multipartite quantum states. We show that, if the measurements are trusted, such inequalities can be used to derive witnesses that can reveal genuine Bell correlations with two collective measurements in systems where many-body correlation functions can be evaluated. This approach, however, utilises the parity measurement which becomes too demanding for large systems, showing also that the approach based on two-body correlations introduces a significant advantage over the other methods. We therefore illustrate how our two-body Bell inequality is associated to a witness that can be successfully applied to already available experimental data from a Bose-Einstein condensate.

Our results pave the way to a more refined study of Bell correlations in many-body systems, by presenting the first available techniques to determine the amount of particles sharing Bell correlations in these systems. Moreover, we stress that our results can already be applied to experimentally detect in a Bell test genuine multipartite nonlocality for systems of size up to $N = 7$. In particular, since the inequalities that we introduce consist only of two-body correlators, such detection would require only an $\mathcal{O}(N^2)$ amount of measurements, contrarily to already known inequalities, such as Mermin's, that involve measuring an exponential amount of correlators.

As a future direction to investigate, it would be interesting to derive inequalities that test for higher nonlocality depth than 6, as it is already possible to do in the case of entanglement. In particular, a more ambitious direction would be to find ways to assess genuine Bell correlations in systems of hundreds of particles without relying on parity measurements. This would give a convenient way to prove that all the particles in the system are genuinely sharing Bell correlations.

As it is argued in the previous sections, the main challenge for these purposes consists in characterising the no-signalling set of multipartite correlations in the subspace of two-body permutationally invariant correlators. We are able to do so only for the cases of low number of parties, while a general and efficient method is still missing. Therefore, a more technical but still interesting question would be to find such a general characterisation.

Chapter 5

Scalable Bell inequalities for qubit graph states and robust self-testing

Bell inequalities constitute a key tool in quantum information theory: they not only allow one to reveal nonlocality in composite quantum systems, but, more importantly, they can be used to certify relevant properties thereof. In this Chapter we provide a general construction of Bell inequalities that are maximally violated by the multiqubit graph states and can be used for their robust self-testing. Apart from their theoretical relevance, our inequalities present two main advantages from an experimental viewpoint: (i) they present a significant reduction of the experimental effort needed to violate them, as the number of correlations they contain scales only linearly with the number of observers; (ii) they allows us to derive robust fidelity bounds for the self-testing of graph states that can be realistically met by present experimental data. We also discuss possible generalisations of our approach to entangled states whose stabilizers are not tensor products of Pauli matrices. The results of this Chapter are based on the original work published in [BAŠ+18].

5.1 Introduction

A very relevant application of Bell nonlocality is self-testing: as discussed in Section 2.3.4, it can be seen as a way of certifying both the state produced and the local measurements performed by some given quantum devices, by simply looking at the resulting correlations. Such a tool is particularly interesting because it offers a way to guarantee that a quantum device is working properly without the need of knowing its internal func-

tioning. It thus consitutes a form of device-independent certification that can be useful for various quantum information protocols. In fact, since its introduction in [MY04], self-testing has been studied in many contexts, showing to be applicable to multipartite states [McK11, ŠCAA18] and any number of measurements as well [ŠASA16]. Moreover, extensions to several different scenarios have also been considered, such as steering [ŠH16], the prepare-and measure framework [TKV$^+$18], networks [BŠCA18a, BŠCA18b] and the certification of quantum channels [SBWS18].

From an implementation perspective, a relevant challenge is to design self-testing strategies that can be applied to realistic situations. Since recent experiments are capable of addressing already tens of particles [WLH$^+$18b, FMM$^+$18] a crucial ingredient for a certifying strategy is to present an efficient scaling in terms of the required resources. Indeed, any method that is based on the full information about either the state or the observed correlations is bound to become intractable already for medium-large systems, since such information scales exponentially with the number of particles involved.

Interestingly, it has already been shown that nonlocality can be assessed with the knowledge of few-body correlations only. As extensively discussed in Chapter 3 and 4, restricting to such partial information is not only appealing for experimental implementations, but it also allows one to devise scalable methods for nonlocality detection in multipartite systems. Moreover, in Chapter 4 we showed that few-body correlations are even enough to make quantitative statements about the nature of nonlocality in many-body systems, such as the estimation of how many particles genuinely share nonlocal correlations among each other. All the above-mentioned techniques require either performing a polynomial scaling number of measurements or the estimation of few collective measurements only. Remarkably, these simplifications already openend the way to the first experimental detections of Bell correlations in many-body systems of hundreds [SBA$^+$16] and hundreds of thousands of atoms [EKHK17].

Since nonlocality is a necessary ingredient for self-testing of multipartite states, a relevant question to ask is which classes of such states can be self-tested using a polynomial amount of information about the observed correlations. In this Chapter we address this question by focusing on graph states, one of the most representative families of multipartite entangled states that include, e.g., GHZ and cluster states. We introduce the first scalable self-testing method for graph states based on Bell inequalities. This implies introducing a new family of Bell inequalities maximally violated by graph states whose violation, contrary to previous

constructions [GTHB05, TGB06, GC08], can be estimated by measuring a number of correlations that scales linearly with the particle number. While other works have already proven self-testing for these states with a similar amount of information [McK11, ŠCAA18] the novelty of our result is the connection to the violation of Bell inequalities. This, *via* the techniques of [Kan16], allows us to make our self-testing statements robust, which is crucial for their experimental implementation.

To construct our Bell inequalities we do not follow the standard approach based on the geometry of the set of correlations admitting local-hidden-variable models. Instead, we exploit the quantum properties of the states and measurements to be certified. A similar approach was used in [SAT+17, KŠT+18] to derive bipartite Bell inequalities maximally violated by maximally entangled states. Remarkably, our method is the first that can systematically derive self-testing inequalities tailored to multipartite states of arbitrary number of particles, based on the knowledge of their stabilizers only. Furthermore, the range of application of our techniques is not limited to the case of graph states, as we demonstrate by deriving Bell inequalities useful for the self-testing of the partially entangled GHZ state.

5.2 CHSH-like Bell inequalities for graph states

Before presenting our results, we first set up the scenario and recall the relevant notation and terminology. We consider the simplest N-partite Bell scenario, referred to as $(N, 2, 2)$ scenario, in which N distant observers share some N-partite quantum state $|\psi\rangle$. On their share of the state, observer i measures one of two dichotomic observables: for further convenience we represent them in the expectation value form $M_{x_i}^{(i)} = M_{x_i}^0 - M_{x_i}^1$ with $x_i = 0, 1$ and $i = 1, \ldots, N$, so to have operators whose outcomes are ± 1 (in the few-party case we will also denote the observables by A_i, B_i etc.). The correlations obtained in this experiment are described by a collection of expectation values

$$\langle M_{x_{i_1}}^{(i_1)} \ldots M_{x_{i_k}}^{(i_k)} \rangle = \langle \psi | M_{x_{i_1}}^{(i_1)} \otimes \ldots \otimes M_{x_{i_k}}^{(i_k)} | \psi \rangle \tag{5.1}$$

which are usually referred to as correlators and we arrange them for our convenience in a vector $\vec{c}$.

Since we are interested in defining Bell inequalities for multi-qubit graph states, let us recall how these states are defined, following what we outlined in Section 2.2.4. Consider a graph $G = (V, E)$, where V is the set of vertices of size $|V| = N$, and E is the set of edges connecting the vertices. Let then $n(i)$ be the neighbourhood of the vertex i, i.e., all

vertices from V that are connected with i by an edge. Now, to every vertex i we associate an operator

$$G_i = X_i \otimes \bigotimes_{j \in n(i)} Z_j, \tag{5.2}$$

in which the X operator acts on site i, while the Z operators act on all sites that belong to $n(i)$. Then, the graph state $|\psi_G\rangle$ associated to G is defined as the unique eigenstate of all these operators G_i $(i = 1, \ldots, N)$ with eigenvalue one. The G_i's are called stabilizing operators of $|\psi_G\rangle$ and they generate the 2^N-element commutative group of operators stabilizing $|\psi_G\rangle$, called *stabilizer group*.

The simplest example of a graph state, corresponding to the two-vertex complete graph up to local unitary equivalence, is precisely the maximally entangled state of two qubits $|\phi_+\rangle$ presented in (2.28). Recall that, as shown in Section 2.3.5, the maximally entangled two-qubit state is the one achieving the maximal violation of the CHSH inequality

$$I_{\text{CHSH}} := \langle (A_0 + A_1)B_0 \rangle + \langle (A_0 - A_1)B_1 \rangle \leq 2, \tag{5.3}$$

Interestingly, there is a direct relation between the stabilizing operators of $|\phi_+\rangle$ and the maximal quantum violation of the CHSH Bell inequality. Precisely, the observables realising the maximal quantum violation of the CHSH Bell inequality can be combined to obtain $(A_0 + A_1) \otimes B_0 = \sqrt{2} X_1 \otimes X_2$ and $(A_0 - A_1) \otimes B_1 = \sqrt{2} Z_1 \otimes Z_2$, which constitute, up to a constant factor, the stabilizing operators of $|\phi_+\rangle$. This is exactly the relation that we exploit below to construct Bell inequalities for graph states. In fact, these inequalities can be seen as a generalisation of the CHSH Bell inequality to the multipartite case. As we explain later, this connection allows to generalise the techniques used to self-test the $|\phi_+\rangle$ state from the maximal violation of CHSH to a self-testing statement for any graph state.

First, let us introduce the new family of Bell inequalities maximally violated by the graph states. Given a graph G we enumerate its vertices, for further convenience, so that the first one has the largest neighbourhood, that is, $|n(1)| = \max_i |n(i)| \equiv n_{\max}$. If there are more vertices with maximal neighbourhood in G, we choose any of them as the first vertex.

Then, to every stabilizing operator G_i corresponding to the graph G we associate an expectation value in which the respective operators are replaced by quantum dichotomic observables or combinations thereof. More precisely, at the first site X_1 and Z_1 are replaced by, respectively, $M_0^{(1)} + M_1^{(1)}$ and $M_0^{(1)} - M_1^{(1)}$, whereas for the remaining observers, X_j

and Z_j are replaced simply by $M_0^{(j)}$ and $M_1^{(j)}$. Finally, if there is an identity at any position in G_i we leave it as it is.

We then add the obtained correlators, multiplying the first one by $n_{\max}$, and obtain the following Bell inequality

$$\begin{aligned} I_G : \;=\; & n_{\max} \left\langle (M_0^{(1)} + M_1^{(1)}) \prod_{i \in n(1)} M_1^{(i)} \right\rangle \\ & + \sum_{i \in n(1)} \left\langle (M_0^{(1)} - M_1^{(1)}) M_0^{(i)} \prod_{j \in n(i) \setminus \{1\}} M_1^{(j)} \right\rangle \\ & + \sum_{i \notin n(1) \cup \{1\}} \left\langle M_0^{(i)} \prod_{j \in n(i)} M_1^{(j)} \right\rangle \leq \beta_G^C. \end{aligned} \tag{5.4}$$

Notice that I_G coincides with the CHSH Bell expression for $N = 2$. Similarly, for higher N it can be seen as a sum of $n_{\max}$ CHSH Bell expressions between the first party and some joint measurements on the parties corresponding to the neighbouring vertices, plus some number of correlators in which the first observer does not appear. This simple structure makes our Bell inequalities extremely easy to characterise. In fact, as shown below, their maximal classical and quantum values can even be computed by hand.

Fact 1. *For a given graph G, the classical bound of the corresponding Bell inequality (5.4) is $\beta_G^C = N + n_{\max} - 1$.*

Proof. We start by noting that (5.4) consists of a single term containing $M_0^{(1)} + M_1^{(1)}$ appearing with weight $n_{\max}$, and $n_{\max}$ different terms containing $M_0^{(1)} - M_1^{(1)}$. Now, for any local deterministic correlations that assign ± 1 to all observables $M_{x_j}^{(j)}$, these two combinations are either zero or two and if one equals two, the other vanishes. Thus, the contribution from these terms to the classical bound is exactly $2n_{\max}$. Then, the maximal value of the remaining correlators in (5.4) over local deterministic strategies is $N - n_{\max} - 1$, which together with the first contribution results in $\beta_G^C = N + n_{\max} - 1$. □

Fact 2. *For a given graph G, the maximal quantum violation of (5.4) is $\beta_G^Q = (2\sqrt{2} - 1)n_{\max} + N - 1$.*

Proof. We first demonstrate that β_G^Q upper bounds the maximal quantum value of (5.4) and then provide an explicit quantum strategy achieving this bound.

Let us consider dichotomic observables $M_{x_i}^{(i)}$ for each observer and construct from them the Bell operator corresponding to the Bell expression I_G,

$$\begin{aligned}\mathcal{B}_G : \;=\; & n_{\max}(M_0^{(1)} + M_1^{(1)}) \otimes \bigotimes_{i\in N(1)} M_1^{(i)} \\ & + \sum_{i\in N(1)} (M_0^{(1)} - M_1^{(1)}) \otimes M_0^{(i)} \otimes \bigotimes_{j\in N(i)\setminus\{1\}} M_1^{(j)} \\ & + \sum_{i\notin N(1)\cup\{1\}} M_0^{(i)} \otimes \bigotimes_{j\in N(i)} M_1^{(j)}, \end{aligned} \tag{5.5}$$

By direct checking it is not difficult to see that the shifted Bell operator $\beta_G^Q \mathbb{1} - \mathcal{B}_G$ can be decomposed into the following sum of squares

$$\begin{aligned}\beta_G^Q \mathbb{1} - \mathcal{B}_G \;=\; & \frac{n_{\max}}{\sqrt{2}} (\mathbb{1} - P_1)^2 + \frac{1}{\sqrt{2}} \sum_{i\in N(1)} (\mathbb{1} - P_i)^2 \\ & + \frac{1}{2} \sum_{i\notin N(1)\cup\{1\}} (\mathbb{1} - P_i)^2 , \end{aligned} \tag{5.6}$$

where P_i are operators defined as

$$P_1 = \frac{M_0^{(1)} + M_1^{(1)}}{\sqrt{2}} \otimes \bigotimes_{i\in N(1)} M_1^{(i)}, \tag{5.7}$$

$$P_i = \frac{M_0^{(1)} - M_1^{(1)}}{\sqrt{2}} \otimes M_0^{(i)} \otimes \bigotimes_{j\in N(i)\setminus\{1\}} M_1^{(j)} \tag{5.8}$$

for $i \in N(1)$, and, finally,

$$P_i = M_0^{(i)} \otimes \bigotimes_{j\in N(i)} M_1^{(j)} \tag{5.9}$$

for $i \notin N(1) \cup \{1\}$. This immediately implies that $\beta_G^Q \mathbb{1} - \mathcal{B}_G \succeq 0$, and since the decomposition (5.6) holds true for any choice of local observables $M_{x_i}^{(i)}$, we have that β_G^Q upper bounds the maximal quantum value of I_G, that is,

$$\max_{Q_N} I_G \leq \beta_G^Q. \tag{5.10}$$

To prove that (5.10) turns into an equality, let us consider the following observables

$$M_0^{(1)} = \frac{1}{\sqrt{2}}(X + Z), \qquad M_1^{(1)} = \frac{1}{\sqrt{2}}(X - Z) \tag{5.11}$$

for the first observer and $M_0^{(i)} = X$ and $M_1^{(i)} = Z$ for $i = 2, \ldots, N$. By a direct check one sees that for these observables and the graph state $|\psi_G\rangle$ the value of I_G is exactly β_G^Q, which completes the proof. □

A few comments are in order. First, it follows that for any graph G, our Bell inequalities are non-trivial, i.e., the maximal quantum violation β_G^Q is always strictly bigger than the local bound β_G^C. Second, it is also interesting to compare our inequalities to previous constructions of Bell inequalities for graph states. The most general one was introduced in [GTHB05] and then modified in [TGB06] to allow for two measurements at all sites. One of the key properties of the inequalities of Refs. [GTHB05, TGB06] is that the ratio between their maximal quantum and classical values is exponential in N, making them robust against experimental imperfections. However, this last feature is only possible due to the fact that the amount of expectation values they contain grows exponentially with N, which certainly makes them highly impractical for experiments involving large number of parties. In contrast, our Bell inequalities have a much simpler structure. In particular, they require measuring only $N - n_{\max} - 1$ expectation values, which results in an exponential reduction in the experimental effort needed to violate them. The price to pay is, however, that the ratio β_G^Q/β_G^C tends to a constant for large N (also when $n_{\max}$ depends on N).

5.3 Two examples

Let us now illustrate our construction with two examples. The first one concerns the star graph presented in Fig. 5.1.a. For this graph $|n(1)| = n_{\max} = N - 1$ and the stabilizing operators are of the form: $G_1 = X_1 Z_2 \ldots Z_N$ for the first vertex and $G_i = X_i Z_1$ with $i = 2, \ldots, N$ for the remaining ones. For our convenience, we apply the Hadamard gate to all the vertices but the first one, which gives us an equivalent set of operators: $G'_1 = X_1 \ldots X_N$ and $G'_i = Z_1 Z_i$ with $i = 2, \ldots, N$. It follows that they stabilise the N-qubit GHZ state

$$|\mathrm{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \tag{5.12}$$

Let us then associate expectation values to each G'_i. As the first vertex is the one with the largest neighbourhood, we make the assignments

$$\begin{aligned} G'_1 &\rightarrow \langle (M_0^{(1)} + M_1^{(1)}) M_0^{(2)} \ldots M_0^{(N)} \rangle \\ G'_i &\rightarrow \langle (M_0^{(1)} - M_1^{(1)}) M_1^{(i)} \rangle \qquad (i = 2, \ldots, N) \end{aligned} \tag{5.13}$$

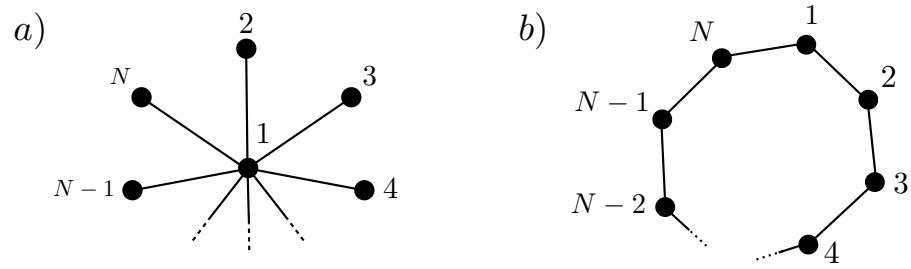

Figure 5.1: Two examples of graphs: (a) the star graph and (b) the ring graph.

which leads us to the following Bell inequality

$$\begin{aligned} \mathcal{I}^N_{GHZ} &= (N-1)\left[\langle M_0^{(1)} M_0^{(2)} \ldots M_0^{(N)}\rangle + \langle M_1^{(1)} M_0^{(2)} \ldots M_0^{(N)}\rangle)\right] \\ &\quad + \sum_{i=2}^{N} (\langle M_0^{(1)} M_1^{(i)}\rangle - \langle M_1^{(1)} M_1^{(i)}\rangle) \leq 2(N-1). \end{aligned} \tag{5.14}$$

Notice that this inequality coincides with Eq. (3.11), which we found numerically from the dual SDP of the nonlocality detection method presented in Chapter 3. Interestingly, this inequality can be interpreted as a sum of $N-1$ CHSH Bell inequalities between the first observer and the remaining ones; for $N=2$ it reproduces the CHSH inequality. It follows from Fact 2 that $\beta^Q_{\mathrm{GHZ}} = 2\sqrt{2}(N-1)$ and it is achieved by the GHZ state (5.12). It should be noticed that contrary to the well-known Mermin Bell inequality [Mer90] which is also maximally violated by this state, our inequality contains a number of correlators that scales linearly with N. Moreover, only two of them are N-body and they involve two different measurements choices only for the first party. All this makes our inequality for the GHZ state more advantageous from the experimental point of view.

As a second example we consider the ring graph presented in Fig. 5.1, for which the stabilizing operators are $G_i = Z_{i-1} X_i Z_{i+1}$ with $i = 1, \ldots, N$, where we use the convention that $Z_0 \equiv Z_N$ and $Z_{N+1} \equiv Z_1$.

As every vertex in this graph has neighbourhood of the same size, i.e., $n(i) = n_{\max} = 2$ $(i = 1, \ldots, N)$, we choose the first vertex to be the one at which we introduce combinations of observables. Thus, following our

recipe,

$$\begin{aligned} G_N &\to \langle M_1^{(N-1)} M_0^{(N)} (M_0^{(1)} - M_1^{(1)}) \rangle \\ G_1 &\to \langle M_1^{(N)} (M_0^{(1)} + M_1^{(1)}) M_1^{(2)} \rangle \\ G_2 &\to \langle (M_0^{(1)} - M_1^{(1)}) M_0^{(2)} M_1^{(3)} \rangle \end{aligned} \tag{5.15}$$

and $G_i \to \langle M_1^{(i-1)} M_0^{(i)} M_1^{(i+1)} \rangle$ for $i = 3, \ldots, N-1$. These expectation values give rise to the following Bell inequality

$$\begin{aligned} I_{\text{ring}} \;:=\; & 2\langle M_1^{(N)} (M_0^{(1)} + M_1^{(1)}) M_1^{(2)} \rangle + \langle (M_0^{(1)} - M_1^{(1)}) M_0^{(2)} M_1^{(3)} \rangle \\ & + \langle M_1^{(N-1)} M_0^{(N)} (M_0^{(1)} - M_1^{(1)}) \rangle \\ & + \sum_{i=3}^{N-1} \langle M_1^{(i-1)} M_0^{(i)} M_1^{(i+1)} \rangle \leq N + 1, \end{aligned} \tag{5.16}$$

whose classical bound stems directly from Fact 1, while, according to Fact 2, its maximal quantum violation is $N + 4\sqrt{2} - 3$ and is achieved by the so-called N-qubit ring cluster state stabilized by the above G_i. Remarkably, this Bell inequality contains only three-body nearest-neighbour correlators, i.e., correlators of minimal length able to detect nonlocality of the ring state. Indeed, as proven in Ref. [GHG10], one cannot detect entanglement of graph states only from their two-body marginals as they are compatible with separable states.

Lastly, notice that in this second example the ratio β_G^Q / β_G^C tends to 1 in the limit of large N, making the violation very sensitive to experimental errors for big systems. This issue can be fixed by properly modifying the inequality with the addition of substitutions $X_j, Z_j \to (M_0^{(j)} \pm M_1^{(j)})$ on other vertices j whose neighbourhood doesn't overlap with $n(1)$ (see Appendix C.1 for a detailed explanation of the generalised method).

5.4 Robust self-testing

Apart from being convenient from the experimental point of view, the introduced Bell inequalities also find applications in self-testing. To recall the task of self-testing, imagine a quantum device that performs a Bell test with some quantum state $|\bar{\psi}\rangle$ and quantum observables $\bar{M}_{x_i}^{(i)}$, producing correlations $\vec{c}$. The aim of self-testing is to reveal the structure of the system $\{|\bar{\psi}\rangle, \bar{M}_{x_i}^{(i)}\}$ from the properties of the observed correlations $\vec{c}$. In particular, here we focus on self-testing through Bell violations, which, as explained in Section 2.3.4, consists in making self-testing statements based solely on the fact that the correlations $\vec{c}$ achieve the maximal quantum violation of a given Bell inequality.

More specifically, we can prove the following fact:

Fact 3. *Given a graph G, if the corresponding Bell inequality (5.4) is violated maximally by a state $|\psi\rangle$ and observables $\bar{M}_j^{(i)}$, then the following holds true:*

$$\Phi[(\bar{M}_{k_{i_1}}^{(i_1)} \otimes \ldots \otimes \bar{M}_{k_{i_1}}^{(i_1)})\,|\psi\rangle] = (M_{k_{i_1}}^{(i_1)} \otimes \ldots \otimes M_{k_{i_1}}^{(i_1)})\,|\psi_G\rangle \otimes |\mathrm{aux}\rangle, \quad (5.17)$$

where $\Phi = \Phi_1 \otimes \ldots \otimes \Phi_N$ with Φ_i being the SWAP isometry represented in Fig. 2.7, $|\mathrm{aux}\rangle$ is some state encoding uncorrelated degrees of freedom,

$$M_j^{(1)} = \frac{1}{\sqrt{2}}[X + (-1)^j Z] \quad (5.18)$$

and

$$M_0^{(i)} = X, \quad M_1^{(i)} = Z \quad (i = 2, \ldots, N). \quad (5.19)$$

Proof. The proof is in Appendix C.2. □

It should be noticed here that, compared to other self-testing methods for graph states, we present the first method that exploits the maximal violation of a multipartite Bell inequality. Moreover, with the aid of the approach developed in [Kan16] our Bell inequalities allow one to make robust self-testing statements.

Let us recall the main ingredients of the method, as outlined in Section 2.3.4: suppose that, upon performing measurements on an unknown quantum state ρ_N, one has observed a value β_{obs} for the violation of the inequality (5.4) for a given graph G. Our aim is to derive a lower bound on the fidelity of the following form

$$\Theta(\rho_N \to \psi_G) \geq s\beta_{obs} + \mu\,, \quad (5.20)$$

for some $s, \mu \in \mathbb{R}$ and where $\Theta(\rho_N \to \psi_G)$ is the fidelity between the measured state and the target graph state $|\psi_G\rangle$ as defined in Eq. (2.52). To this end, recall that it is enough to prove the operator inequality

$$K := (\Phi_1^\dagger \otimes \ldots \otimes \Phi_N^\dagger)(|\psi\rangle\,\langle\psi|) \geq s\hat{\mathcal{B}}_G + \mu\mathbb{1} \quad (5.21)$$

where $\hat{\mathcal{B}}_G$ is the Bell operator corresponding to the inequality (5.4) and constructed from any possible choice of dichotomic observables $M_{x_i}^{(i)}$. Proving such an operator inequality for arbitrary local observables in $\mathcal{B}_G$ is certainly a formidable task. However, due to the fact that here we consider the simplest Bell scenario involving two dichotomic measurements per site, one can exploit Jordan's lemma, which, as explained in

[Kan16], reduces the problem to basically an N-qubit space. That is, the local observables $M_{x_i}^{(i)}$ can now be parametrised as

$$M_{x_1}^{(1)} = \cos\alpha_1 \, X + (-1)^{x_1} \sin\alpha_1 \, Z, \tag{5.22}$$

and

$$M_{x_i}^{(i)} = \cos\alpha_i \, H + (-1)^{x_i} \sin\alpha_i \, V \tag{5.23}$$

for $i = 2, \ldots, N$, where $H = (X + Z)/\sqrt{2}$, $\sigma_V = (X - Z)/\sqrt{2}$ and $\alpha_i \in [0, \pi/2]$. This gives rise to a Bell operator $\mathcal{B}_G(\vec{\alpha})$ that now depends on the angles α_i. Let us then consider particular quantum channels

$$\Phi_i(\alpha_i)[\rho] = \frac{1 + g(\alpha_i)}{2}\rho + \frac{1 - g(\alpha_i)}{2}\Gamma_i(\alpha_i)\rho\Gamma_i(\alpha_i)\,, \tag{5.24}$$

where the dependence on the measurement angle is encoded in the function $g(x) = (1 + \sqrt{2})(\sin x + \cos x - 1)$ together with the definition of $\Gamma(x) = N_i^a$ if $x \leq \pi/4$ and $\Gamma(x) = N_i^b$ if $x > \pi/4$. Lastly, we define $N_1^{a,b} = X, Z$ and $N_i^{a,b} = H, V$ for $i = 2, \ldots N$.

We now want to prove that for all possible choices of α_i, the following inequality is satisfied

$$K(\alpha_1, \ldots, \alpha_N) \geq s\mathcal{B}_G(\alpha_1, \ldots, \alpha_N) + \mu\mathbb{1} \tag{5.25}$$

for some choice of $s, \mu \in \mathbb{R}$, which, as exampled earlier, would imply an inequality for the extractability.

To analyse the robustness of our self-testing method for graph states, we have performed numerical tests to derive bounds of the kind (5.25) for the inequality for the GHZ state and the ring cluster state for values of $N \leq 7$. The applied procedure works as follows: given a fixed s, estimate the corresponding μ by numerically computing the minimal eigenvalue of the operator $K + s\mathcal{B}_G$ and minimising over all the angles α_i. Notice that to have a fidelity bound that leads to fidelity 1 at the point of maximal violation, the inequality (5.25) has to become tight for the measurements angles leading to the maximal violation, that is $\alpha_i = \pi/4$ for all $i = 1, \ldots, N$. As a second step, we therefore estimated numerically the minimum value of s for which the corresponding bound still satisfied such a property. This led to linear bounds with the optimal slope.

In fact, the numerical results in Fig. 5.2 show that the fidelity between the state $|\psi\rangle$ violating our inequalities for two exemplary graphs and the corresponding graph state $|\psi_G\rangle$ is a linear function of the value β_{obs} for the observed violation.

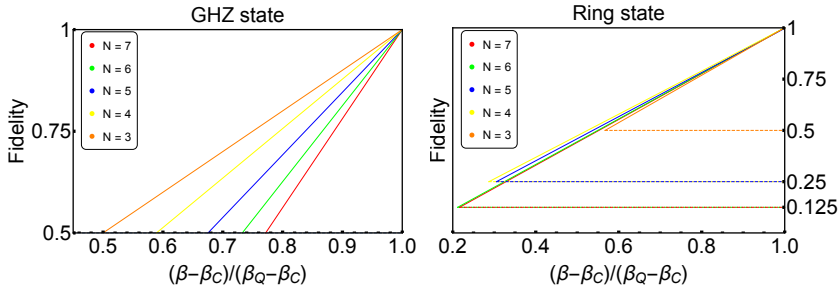

Figure 5.2: Fidelity with the target graph state, numerically estimated as a function of the relative observed violation $(\beta - \beta_C)/(\beta_Q - \beta_C)$ of the corresponding Bell inequalities (5.14) and (5.16) constructed with our method. The plots show the case of a GHZ state (left) and ring graph state (right) of $N = 3, \ldots, 7$ particles. The bounds are plotted until the highest value of fidelity with a separable N-partite state, taken from [MMV07]. Indeed, after that threshold, the device-independent fidelity estimation would not witness any non-classicality in the state.

5.5 Generalisation of the method

Interestingly, our construction can be generalised so to work in cases where the stabilizer operators are not products of Pauli operators. To give an example, let us consider the partially entangled GHZ state

$$|\mathrm{GHZ}_N(\theta)\rangle = \cos\theta\,|0\rangle^{\otimes N} + \sin\theta\,|1\rangle^{\otimes N}\ , \tag{5.26}$$

with $\theta \in (0, \pi/4]$, whose generators of the stabilizer group can be chosen to be

$$\begin{aligned} G_1(\theta) &= \sin 2\theta X_1 X_2 \ldots X_N + \cos 2\theta Z_1\ , \\ G_i &= Z_1 Z_i\ , \quad i = 2, \ldots, N. \end{aligned} \tag{5.27}$$

The partially entangled GHZ state is not a graph state and, indeed, contrarily to the case of graph states, the operator $G_1(\theta)$ can not be decomposed as a product of local Pauli operators. In fact, although $G_1(\theta)$ is unitary, it can not even be expressed as a product of generic local unitaries $U^{(1)} \otimes \ldots \otimes U^{(N)}$. One can see that by computing its action on the GHZ state (5.12), leading to

$$G_1(\theta)\,|GHZ_N\rangle = \frac{\sin 2\theta + \cos 2\theta}{\sqrt{2}}\,|0\rangle^{\otimes N} + \frac{\sin 2\theta - \cos 2\theta}{\sqrt{2}}\,|1\rangle^{\otimes N}\ , \tag{5.28}$$

which, being another partially entangled GHZ state, is locally-unitary-inequivalent to the maximally entangled GHZ state.

To construct a Bell inequality maximally violated by (5.26), we interpret the previous construction for graph states as a special instance of a more general method. The idea is to associate, as before, an expectation value to each stabilizing operator G_i: for the first party we substitute

$$X_1 \to \frac{M_0^{(1)} + M_1^{(1)}}{2\sin\mu}, \qquad Z_1 \to \frac{M_0^{(1)} - M_1^{(1)}}{2\cos\mu}, \tag{5.29}$$

whereas at the remaining sites we traditionally set $X_i \to M_0^{(i)}$ and $Z_i \to M_1^{(i)}$. Having in mind its application to self-testing, we want to obtain a Bell inequality whose associated shifted Bell operator can be decomposed as

$$\beta_Q \mathbb{1} - \mathcal{B} = \sum_{i=1}^{N} \alpha_i^2 (\mathbb{1} - \mathcal{G}_i)^2 \ , \tag{5.30}$$

where the α_i's are generic real numbers and the operators $\mathcal{G}_i$ are polynomials in the measurements operators $M_{x_i}^{(i)}$, obtained from the expression of the stabilizers G_i upon applying the substitutions considered above. In order to derive a valid Bell inequality from (5.30), one has to make sure that the resulting Bell operator corresponds to an inequality that does not contain expectation values that are not measurable, such as terms like $\langle M_0^{(i)} M_1^{(i)} \rangle$. To do so, one can optimize over the $N+1$ free parameters constituted by the coefficients α_i and the angle μ appearing in (5.29).

Remarkably, the outlined procedure is precisely a generalisation of the method we used to derive our inequalities for graph states. To see that, notice that if one takes as stabilizers those in Eq. (5.2), by setting $\mu = \pi/4$ the corresponding operators $\mathcal{G}_i$ coincide with the P_i ones that we introduced in Eqs. (5.7 – 5.9). Moreover, the SOS (5.30) recovers the decomposition for the inequality $\mathcal{I}_G$, presented in Eq. (5.6), if one chooses as coefficients $\alpha_1 = n_{max}/\sqrt{2}$, $\alpha_i = 1/\sqrt{2}$ for $i \in N(1)$ and $\alpha_i = 1/2$ for the rest.

Let us now show how the same procedure can also be applied to the case of the partially entangled GHZ state. As we prove in Appendix C.2, we obtain a valid Bell operator from the SOS decomposition from (5.30) by choosing the angle μ such that $2\sin^2\mu = \sin^2 2\theta$ and the coefficients as $\alpha_1^2 = \sqrt{2}(N-1)$ and $\alpha_2^2 = \ldots = \alpha_N^2 = \sqrt{2}$. The corresponding Bell

inequality reads as follows

$$\begin{aligned}\mathcal{I}_\theta \;:=\; & (N-1)\langle (A_0^{(1)}+A_1^{(1)})A_0^{(2)}\dots A_0^{(N)}\rangle \\ & +(N-1)\frac{\cos 2\theta}{\sqrt{1+\cos^2 2\theta}}(\langle A_0^{(1)}\rangle - \langle A_1^{(1)}\rangle) \\ & +\frac{1}{\sqrt{1+\cos^2 2\theta}}\sum_{i=2}^{N}\langle (A_0^{(1)}-A_1^{(1)})A_1^{(i)}\rangle \leq \beta_C\,, \end{aligned} \tag{5.31}$$

where the classical bound amounts to

$$\beta_C(\theta) = 2(N-1)\frac{1+\cos 2\theta}{\sqrt{1+\cos^2 2\theta}}. \tag{5.32}$$

and the corresponding maximal quantum violation, achieved by the partially entangled GHZ state, to

$$\beta_Q = 2\sqrt{2}(N-1) \tag{5.33}$$

for all values of $\theta \in (0, \pi/4]$. Moreover, in Appendix C.2 we prove that this inequality can be used to self-test the partially entangled GHZ state for any $\theta \in (0, \pi/4]$ and any number of particles N. Noticeably, the case $\theta = \pi/4$ recovers the inequality (5.14) for the GHZ state. Let us also notice that for $N = 2$ we obtain a Bell inequality maximally violated by any pure entangled state, which is inequivalent to the well-known tilted CHSH Bell inequality [AMP12, BP15].

5.6 Discussion

We have introduced a family of Bell inequalities that are maximally violated by the graph states and are scalable from an experimental point of view. That is, contrary to the previous constructions of Bell inequalities for graph states, the number of expectation values they contain grows only linearly in the number of parties. Furthermore, the extremely simple structure of our Bell inequalities makes them easily applicable to robust self-testing.

Our considerations provoke further questions. First, it would be interesting to see whether the approach presented here can be generally applied to entangled states stabilized by operators that are not just products of Pauli matrices. Here we showed that such generalisation is possible for partially entangled GHZ states. Second, it would be of interest to investigate whether this approach can be exploited for multipartite states of higher local dimensions; in particular, the multiqudit graph states,

for which no Bell inequalities are known. Let us also mention that another method to derive Bell inequalities from stabilizing formalism was presented in [SBWS18]. One could explore possible connections between both approaches.

Chapter 6

Verification of Quantum Optimizers

Solving optimisation problems encoded in the ground state of classical-spin systems is a focus area for existing quantum computing devices. Their outputs provide upper bounds to the unknown ground-state energy. To certify these bounds, they are compared to those obtained by classical methods. However, even if the quantum bound beats any classical bound, this says little about how close it is to the actual solution. In this Chapter, we consider relaxations to the ground-state problem based on semidefinite programming to benchmark quantum optimisers. These relaxations are radically more informative because they provide lower bounds to the ground-state energy. The method also provides upper bounds with little additional cost. We verify the output of a D-Wave 2000Q device and identify instances where our method provides the exact ground state, while the annealer gives a configuration of higher energy. This new tool provides a scalable certification of existing and near-future quantum devices for combinatorial optimisation. The results of this Chapter are based on the original work published in [BGWA18].

6.1 Introduction

Classical Ising models are among the most paradigmatic and widely studied models in statistical physics. They are capable of describing an immense variety of interesting physics, ranging from ferromagnetic to frustrated and glassy phases. Moreover, they are important in fields as diverse as risk assessment in finance, logistics, machine learning [KFGT07], and image de-noising [BD94] because the solution of many optimisation and decision problems, such as partitioning, covering, and satisfiability can

be encoded in the ground state of such models [Luc14]. Their generality and the exponentially growing spaces of spin configurations, however, preclude the existence of any efficient general purpose algorithm to obtain the ground state. It is hence no surprise that a wealth of approximate but more scalable classical techniques for the energy minimisation in such models have been developed.

Recently, novel approaches that leverage the power of near-term quantum devices such as quantum annealers, variational quantum eigensolvers [PMS$^+$14], variational circuits [FGG14, Cro18] or networks of degenerate optical parametric oscillators [QNN17], are proposed for performing such tasks [DBI$^+$16][CH16][MK18]. Their quality is usually benchmarked against some of the most scalable classical approaches, e.g., simulated annealing [KGV83] or variational ansatz classes based on tensor-network states. All of these methods share one common feature: they only provide upper bounds on the ground-state energy. Even when the quantum method beats all classical ones, there is no guarantee that the upper bound of the quantum device is actually close to the true ground-state energy. To overcome this limitation, it is important to develop schemes that provide reliable lower bounds to the ground-state energy of spin problems, against which the results of quantum devices, and also classical variational methods, can be compared.

Here we tackle this issue by leveraging the relaxations of polynomial optimisation problems through semidefinite programming (SDP) presented in Section 2.1.4. The proposed method provides lower bounds on the ground-state energy by optimizing over a larger set than the physical spin configurations. We improve the scalability of this type of relaxation, by introducing a method known as the chordal extension [WKKM06, Las06], which allows us to exploit the physical locality and sparsity structure present in relevant problem instances. All in all, this yields an increasingly precise hierarchy of rigorous lower – in fact also upper – bounds on the ground state energy. Combining these bounds in a branch-and-bound (BB) scheme (see for instance [RRW08] for a recent summary of these techniques), we obtain a scalable and flexible method for the computation of certified ground state energies and configurations.

How can one find the lowest energy configuration among the more than 10^{360} possible configurations of a typical Ising model with, say 35×35 sites? The key is to compute a converging series of upper and lower bounds on the ground state energy and use these bounds to drastically reduce the search space that needs to be explored. Configurations that fall outside the band between the bounds no longer need to be explored. This is precisely the strategy of the BB approach (see from Figure 6.1). Obtaining good lower bounds is the non-trivial part and several

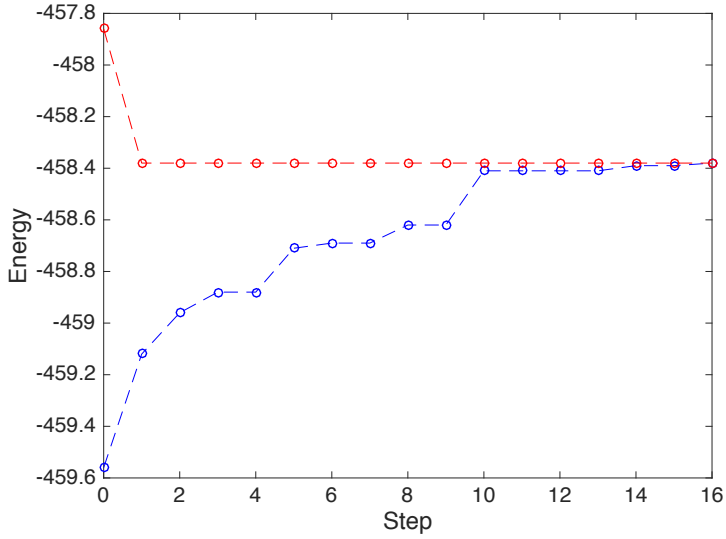

Figure 6.1: Example of sequences of upper and lower bounds obtained with our method for a 2D Ising model of lattice size 15×15. Due to the combinations of bounds from below and above, our approach ultimately converges and gives an exact and certified solution for the ground-state energy and configuration. Although the complexity of the general Ising problem implies that one has to run an exponential number of steps to achieve convergence, in many cases it is reached in polynomial time. Here this happens after less than 20 steps, instead of having to explore all of the 2^{225} configurations.

proposals have been considered through the last years: one can generally divide them into techniques based on a linear-programming relaxation [LJRR04] and ones based on semidefinite programming [RRW08]. The former approaches are known to perform better for very sparse graphs, such as 2D square lattices and planar graphs, but it is generally hard to adapt them to deal efficiently with more general problems. On the other hand, the SDP method introduced in [RRW08] applies to general graphs and is always polynomial in the system size (per step), but does not outperform linear programming for very sparse graphs. The chordal branch-and-bound (CBB) method we propose keeps the polynomial dependence on the size, while being both more efficient than the BB approach from [RRW08] for sparse instances and readily applicable to less sparse Ising models. It is therefore a good candidate for the verification of current and near future quantum optimisation devices.

Due to the combinations of bounds from below and above, any BB

technique ultimately converges to the lowest achievable energy and outputs a corresponding configuration that achieves it. It thereby gives an exact and certified solution to the ground state problem. Although the complexity of the problem implies that, at least in some cases, one has to run an exponential amount of steps to achieve convergence, in many scenarios convergence is reached after a polynomial number of steps and then the method is efficient (the complexity per step and number of required steps can be tuned by adjusting the level of the relaxation, as we will see later). Even in cases where convergence cannot be achieved with the available computational resources, the obtained lower and upper bounds still imply an interval in which the true ground state energy must provably lie. This fundamentally differentiates both BB and CBB from techniques such as simulated annealing or variational methods, which can reach larger system sizes, but provide not strong certificate for the solutions they propose.

6.2 Preliminaries

Before describing the techniques we combine in more detail, we first introduce the relevant concept and notation on classical Ising models. Moreover, we review what is known about the complexity of the ground state problem and point out the consequences this has for the benchmarking of quantum optimizers.

6.2.1 Setting and notation

We consider classical spin systems whose configurations $\vec{\sigma} \coloneqq (\sigma_1, \ldots, \sigma_N)$ are vectors of N spin variables $\sigma_i \in \{-1, 1\}$ to each of which a Hamiltonian H assigns an energy $H(\vec{\sigma})$. We are mostly interested in Hamiltonians of Ising type, that can be written in the form

$$H(\vec{\sigma}) = -\sum_{1 \leq i < j \leq N} J_{ij}\sigma_i\sigma_j + \sum_{i=1}^{N} h_i\sigma_i, \tag{6.1}$$

with couplings J_{ij} and local fields h_i, but the method we develop is more general and can also be applied to Hamiltonians that are higher order polynomials of the σ_i and couple three or more spins in a single term.

Many spin models of interest in physics and beyond are characterised by a locality structure, i.e., not all the spins interact with each other so that some J_{ij} are zero. Such locality of interactions implies a sparsity of the resulting Hamiltonian and hence optimisation problem. This locality and sparsity can be most efficiently captured in the language of graph

theory: we define the interaction (hyper-)graph as the graph $\mathcal{G} \coloneqq (\mathcal{V}, \mathcal{E})$ whose vertex set $\mathcal{V} \coloneqq \{1, \ldots, N\}$ is the set of indices of the spin variables and whose (hyper-)edge set $\mathcal{E}$ is the set of all pairs (or larger subsets) of indices for which the Hamiltonian contains an interaction, i.e., in the above example $\{i, j\} \in \mathcal{E} \iff J_{ij} \neq 0$. More important for us is the dependency graph $G \coloneqq (\mathcal{V}, D)$, which is a related concept but always a graph and not a hyper-graph, namely the one that contains an edge for any pair of indices of spin variables that appear together in the same Hamiltonian term. For the example Hamiltonian (6.1) G and $\mathcal{G}$ are identical, but in general one obtains G by replacing every hyper-edge in $\mathcal{G}$ by a clique, that is a fully connected subgraph. Typical examples of interaction and dependency graphs are regular cubic grids, such as for example in the 1D and 2D Ising model.

Among all the configurations of such a system there are those that achieve the minimal possible energy, also known as the ground state energy and defined as

$$E_g \coloneqq \min_{\vec{\sigma} \in \{-1,1\}^N} H(\vec{\sigma}). \tag{6.2}$$

If only one configuration achieves energy E_g we call this configuration the ground state and say that it is unique, otherwise we call the collection of all configurations with energy E_g the ground state space. For our purposes, solving the ground state problem for a given Hamiltonian means finding E_g and outputting a configuration that achieves it. Obviously, the ground state problem is an optimisation problem that can, in principle, be solved by brute force, by simply computing $H(\vec{\sigma})$ for all possible configurations σ. This however quickly becomes infeasible as the number of configurations grows like 2^N, restricting this approach to systems of size roughly $N \lessapprox 20$.

Therefore, several methods have been proposed to solve the ground state problem more efficiently. However, as we will see in the next Section, several results have been obtained regarding the complexity of such problem, implying that no efficient method can be found to compute the ground state of a general Ising model.

6.2.2 Complexity of finding Ising ground states

There is a wealth of results on the worst case complexity of finding the ground state of various Ising models [GJR87]. Thereby "worst case complexity" is the complexity of the hardest instances within a class of families of problems of increasing size. How hard it is to solve the ground-state problem of such a family varies with the interaction graph and can crucially depend on seemingly unimportant details. We consider Hamil-

tonians that are polynomials (with fixed finite degree and finite precision coefficients) in the spin variables (such as those given in (6.1)) and interaction (hyper-)graph $\mathcal{G} \coloneqq (\mathcal{V}, \mathcal{E})$. The size of a problem is the number of vertices $N \coloneqq |\mathcal{V}|$. We say that an Ising model of the form (6.1) has no fields if $h_i = 0$ for all i, we say it has an external field if all $h_i = h$ for all i and some h, and we say it has on-site fields if all h_i can be chosen independently.

Finding the ground state of Hamiltonians of the form (6.1) for arbitrary graphs is in general NP-hard [Bar82], even without any fields. This is still true for $J_{ij} \in \{-1, 0, 1\}$ and $\mathcal{G}$ a finite 3D cubic grid graph and even for $\mathcal{G}$ a cubic two-layer 2D grid [Bar82]. In contrast, for planar graphs $\mathcal{G}$ and without local fields, the ground state can be found efficiently even without the restriction $J_{ij} \in \{-1, 0, 1\}$ [GJR87]. With the restriction $J_{ij} \in \{-1, 0, 1\}$ this even holds for toroidal graphs (grids on a torus, i.e., systems with periodic boundary conditions) [GJR87]. Similarly, if $J_{ij} \geq 0$, then even some systems with local fields can be solved in polynomial time [GJR87]. On the other hand, for general planar graphs with interactions $J_{ij} = -1$ and uniform external field $h_i = 1$, finding the ground state is again NP-hard [Bar82]. Ref. [GJR87] contains a list of further concrete models whose complexity is either known to be in P or proven to be NP-hard.

These hardness results are typically obtained by reducing the ground state problem to the so-called max-cut problem, which is known to the NP-hard. The polynomial time algorithms to solve the other families of systems, in turn, work by finding perfect matchings [Bar82] or rely on so-called max-flow/min-cut methods [GJR87].

6.3 The chordal branch and bound method

Here we describe the relaxation of the ground state problem that we use to obtain both lower and upper bounds on the ground state energy and how sparsity can be exploited by means of the chordal extension. We then show how the combination of lower and upper bounds can be exploited in a branch and bound algorithm to converge to exact ground state energy. Lastly, we explain in detail how to combine all these ingredients to obtain the proposed chordal branch and bound method.

6.3.1 Main Ingredients

In this section we describe in detail the methods we build upon and the resulting chordal branch and bound algorithm. We begin by introducing

additional notation. A state of an N spin system is a probability distribution P over the set of configurations $\{-1,1\}^N$. For every function $f : \{-1,1\}^N \to \mathbb{R}$ we can then define its expectation value in the state P as

$$\langle f \rangle_P = \sum_{\vec{\sigma} \in \{-1,1\}^N} f(\vec{\sigma})\, P(\vec{\sigma}). \tag{6.3}$$

We call any state P that is supported only on the ground state space of a model a ground state and such P are manifestly those that achieve the minimal possible expectation value for the Hamiltonian, i.e, $\min_P \langle H \rangle_P = E_g$.

A hierarchy of SDP relaxations for the lower and upper bound

Computing the minimal energy of (6.1) can be seen as a degree-two polynomial minimisation problem in the spin variables, where their dichotomy can be imposed by adding the linear constraints $\sigma_i^2 = 1$. Hence, to obtain a lower bound on the ground-state energy we exploit the method pioneered by Lasserre (see Section 2.1.4 for more details) that introduces a hierarchy of relaxation for constrained polynomial optimisation problems. Recall that the key observation to derive Lasserre's hierarchy is to notice that the minimisation of the polynomial $H(\vec{\sigma})$ is equivalent to the minimisation of its expectation value $\langle H \rangle_P$ over any valid probability distribution $P(\vec{\sigma})$ on the spin variables. In a more physical language, those distributions represent exactly all valid states of a spin system.

Let us briefly revise the general method by using the notation here, instead of introducing it in the more typical framework of polynomial optimisation. Recall that, given a vector $\vec{x} \coloneqq (x_\alpha)_{\alpha=1}^k$ of monomials of the spin variables, the corresponding moment matrix $\Gamma(P)$ is defined as the $k \times k$ matrix of expectation values $\Gamma_{\alpha\beta}(P) \coloneqq \langle x_\alpha\, x_\beta \rangle_P$. Notice that, in the scenario we are considering, there is no need to introduce localising matrices. Indeed, all the relevant constrains can be captured inside the moment matrix. Physically, these constraints reflect the two basic properties of classical spin variables of taking dichotomic values $\sigma_i \in \{-1,1\}$ and commuting with each other. For instance, it is not hard to see that these properties imply conditions on the expectation values such as, for example, $\langle \sigma_i \sigma_j \sigma_i \rangle_P = \langle \sigma_j \rangle_P$.

We can now generalise this concept and think of any real symmetric $k \times k$ matrix as an assignment to expectation values of monomials $x_\alpha\, x_\beta$, that need not necessarily be achievable by any physical state P. If the vector $\vec{x}$ contains at least a suitable subset of polynomials of spin variables, one can further compute the expectation value of the Hamiltonian from the entries of the moment matrix in the sense that there is a matrix

h (depending on the J_{ij} and h_i in case the Hamiltonian is of the form in (6.1)), such that for any physical state P it holds that $\langle H\rangle_P = \mathrm{tr}(h\,\Gamma(P))$. If this is the case, one can relax the ground state problem by computing the energy in this way and optimizing over all matrices Γ that are positive semidefinite and fulfil the above mentioned linear constraints, rather than over those that can actually arise from a physical state P.

Recall that a systematic way of constructing a hierarchy of such relaxations is as follows: Let $\vec{x}^{(\nu)}$ be the vector of all monomials of spin variables of degree up to ν. Then (for any sufficiently large ν so that h, implicitly defined via $\forall P\colon \langle H\rangle_P = \mathrm{tr}(h\,\Gamma(P))$, exists), the minimum achievable in the minimisation problem

$$\begin{aligned} E_g^{(\nu)} \quad &= \quad \min_{\Gamma^{(\nu)}} \mathrm{tr}(h\,\Gamma^{(\nu)}) \\ &\text{s.t.} \quad \Gamma^{(\nu)} \succeq 0, \\ &\qquad \mathrm{tr}(F_m \Gamma^{(\nu)}) = 0 \quad , \ \forall m \in \{1,\ldots,k\}\,. \end{aligned} \tag{6.4}$$

Notice that the above equation is the equivalent of (2.19), where the F_m represent the afore-mentioned linear constrains that replace the use of localising matrices. As argued in Section 2.1.4, the hierarchy (6.4) leads to a convergent series $E_g^{(1)} \leq E_g^{(2)} \leq \ldots \leq E_g$ of lower bounds to the ground state energy of H.

Lastly, let us illustrate this relaxation with an example. If we are working at level $\nu = 2$ for a system of $N = 3$ spins, the corresponding Γ matrix takes the following form:

$$\Gamma^{(2)} = \begin{pmatrix} 1 & \langle\sigma_1\rangle & \langle\sigma_2\rangle & \langle\sigma_3\rangle & \langle\sigma_1\sigma_2\rangle & \langle\sigma_1\sigma_3\rangle & \langle\sigma_2\sigma_3\rangle \\ \langle\sigma_1\rangle & 1 & \langle\sigma_1\sigma_2\rangle & \langle\sigma_1\sigma_3\rangle & \langle\sigma_2\rangle & \langle\sigma_3\rangle & \langle\sigma_1\sigma_2\sigma_3\rangle \\ \langle\sigma_2\rangle & \langle\sigma_1\sigma_2\rangle & 1 & \langle\sigma_2\sigma_3\rangle & \langle\sigma_1\rangle & \langle\sigma_1\sigma_2\sigma_3\rangle & \langle\sigma_3\rangle \\ \langle\sigma_3\rangle & \langle\sigma_1\sigma_3\rangle & \langle\sigma_2\sigma_3\rangle & 1 & \langle\sigma_1\sigma_2\sigma_3\rangle & \langle\sigma_1\rangle & \langle\sigma_2\rangle \\ \langle\sigma_1\sigma_2\rangle & \langle\sigma_2\rangle & \langle\sigma_2\rangle & \langle\sigma_1\sigma_2\sigma_3\rangle & 1 & \langle\sigma_2\sigma_3\rangle & \langle\sigma_1\sigma_3\rangle \\ \langle\sigma_1\sigma_3\rangle & \langle\sigma_3\rangle & \langle\sigma_1\sigma_2\sigma_3\rangle & \langle\sigma_1\rangle & \langle\sigma_2\sigma_3\rangle & 1 & \langle\sigma_1\sigma_2\rangle \\ \langle\sigma_2\sigma_3\rangle & \langle\sigma_1\sigma_2\sigma_3\rangle & \langle\sigma_3\rangle & \langle\sigma_2\rangle & \langle\sigma_1\sigma_3\rangle & \langle\sigma_1\sigma_2\rangle & 1 \end{pmatrix} \tag{6.5}$$

The expectation value of any Hamiltonian of the form given in (6.1) can be expressed as a function of the entries of $\Gamma^{(2)}$ as $\langle H\rangle = J_{12}\Gamma^{(2)}_{15} + J_{13}\Gamma^{(2)}_{16} + J_{23}\Gamma^{(2)}_{17} + h_1\Gamma^{(2)}_{12} + h_2\Gamma^{(2)}_{13} + h_3\Gamma^{(2)}_{14}$. Similarly, one can see how the linear constraints F_m on the entries reflect the properties of the spin variables. Dichotomy directly imposes the conditions $\Gamma^{(2)}_{ii} = 1$ on the diagonal variables and, combined with commutations, allows to identify some of the entries, such as for example $\Gamma^{(2)}_{13} = \Gamma^{(2)}_{25}$.

Let us also mention that Lassere himself first explored the application of such a relaxation to the ground state energy problem, expressed

in terms of its max-cut equivalent [Las01a]. Hence, the result hierarchy relies on $0-1$ variables, instead of ± 1 ones. Furthermore, as a comparison with previous branch-and-bound methods, notice that the one introduced in Ref. [RRW08] exploits a lower bound method that is almost equivalent to the first level of the relaxation (6.4), with the addition of some hand crafted linear constraints. Indeed, the mentioned relaxation can be obtained by considering a moment matrix generated by the set of monomials composed of the spin variables only, without the identity operator. Hence, it results in the first level of the Lasserre hierarchy, diminished by the absence of one (the first) row of the matrix. In contrast, the hierarchy discussed here allows to systematically construct an infinite family of increasingly precise relaxations that yield better and better bounds at an increasing computational cost.

Lastly, let us comment that from the solution of the considered relaxation one can also extract a spin configuration with no additional computational cost. Let Γ^* be the optimal solution to the SDP. We can associate to it a configuration $\vec{\sigma}^*$ by taking the sign of the entries in that matrix that correspond to the expectation values $\langle \sigma_i \rangle$, namely set $\sigma_i^* := \mathrm{sign}(\Gamma^*_{1,i+1})$. The energy of that configuration $H(\vec{\sigma}^*)$ clearly provides an upper bound to the ground-state energy.

Exploiting sparsity via the chordal extension

Recall that, depending on the kind of system considered, the optimisation problem defined by the Hamiltonian (6.1) can be sparse. As is shown in Refs. [WKKM06, Las06], one can exploit this sparsity to derive a more scalable relaxation than (6.4). Intuitively, the idea behind the modification is the following: for any pair of non-interacting spins i, j, the corresponding two-body expectation value $\langle \sigma_i \sigma_j \rangle_P$ is not needed for the computation of the energy. Thus, a moment matrix with all two-body correlations is including some potentially unnecessary information. Hence, finding the minimal amount of such information that is sufficient to perform the optimisation of the energy, helps define a more efficient relaxation.

The method works as follows: take the dependency graph G of the problem and check if it is chordal. A graph is said to be chordal if all its cycles of four or more vertices have a chord, i.e. an edge that is not part of the cycle but connects two vertices of the cycle. If G is not chordal, construct a so-called chordal extension G_C of G by suitably adding edges until the graph is chordal (see Figure 6.2 for an example). The chordal extension of a graph is not unique, but a chordal extension can always be found, simply because any fully connected graph is chordal. The challenge

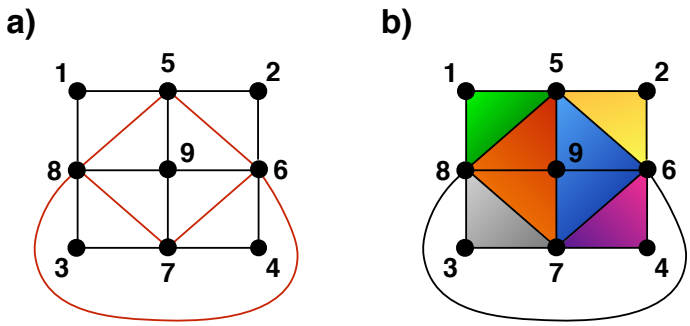

Figure 6.2: a) An example of graph G that is not chordal, together with an option of edges to add (shown in red) in order to obtain a chordal extension G_C. The new edges are chosen to "break" the larger cycles, such as for example the cycle $\{1, 5, 9, 8\}$. b) The graph G_C and its corresponding maximal cliques C_l, shown in the different colors. In this example, the graph has $n_c = 6$ cliques, out of them two are composed of 4 vertices, while the remaining ones consist of 3 vertices each. The G_C is much sparser than a fully connected graph.

is to find a chordal extension that is still relatively sparse. A general polytime technique to find good chordal extensions that worked well for all the cases studied in this Chapter is to compute an approximate minimum degree ordering of the graph nodes, followed by Cholesky factorisation of a positive semidefinite matrix with the associated sparsity pattern [VA15].

Once a specific chordal extension G_C is constructed, it will contain a number of n_C maximal cliques $C_l \subset \mathcal{V}$. A clique, that is a fully connected subgraph, is maximal if it cannot be extended by including any other adjacent vertex. Since the graph G represents a sparse Hamiltonian, and G_C is obtained from G by simply adding some edges, the function (6.1) can be decomposed into a sum $H = \sum_l H_{C_l}$ of terms that each contain only variables contained in a given maximal clique C_l.

One can then modify the optimisation problem in (6.4) as follows: replace the big $\Gamma^{(\nu)}$ matrix by a direct sum of smaller matrices $\Gamma_l^{(\nu)}$, one for each clique, constructed from the spin variables belonging to the clique C_l. Some spin variables appear in more than one clique, which can be captured with additional linear constraints that involve variables of the blocks $\Gamma_l^{(\nu)}$. Writing this explicitly, the chordal version of the SDP relaxation then reads

$$\begin{aligned}
&\min_{\Gamma_l^{(\nu)}} \sum_n \mathrm{tr}(h_n \Gamma_n^{(\nu)}) \\
&\text{s.t.} \quad \Gamma_l^{(\nu)} \succeq 0, \quad \forall\, l = 1, \dots n_C\,, \\
&\qquad \mathrm{tr}(F_{m,l}\Gamma_l^{(\nu)}) = 0 \quad m = 1, \dots, k_l \;, l = 1, \dots n_C\,, \\
&\qquad \sum_n \mathrm{tr}((G_{l,n})\Gamma_n^{(\nu)}) = 0 \quad l = 1, \dots, k\;,
\end{aligned} \tag{6.6}$$

where the $F_{m,l}$ are the intra-block constraints coming from the properties of the spin variables, while the $G_{l,n}$ correspond to the constraints identifying expectation values belonging to different blocks. Interestingly, this relaxation still converges to the exact result, as was shown in [Las06]. Depending on the sparsity of the graph G (and its chordal extension G_C), substituting the original optimisation relaxation (6.4) by (6.6) leads to a substantial simplification and improved scaling in runtime and memory. In practical applications, the latter are typically dominated by the the largest block, i.e., the largest maximal clique in G_C. Moreover, the block-structure can be exploited to have a more finely tuned control of the lower bound precision, essentially by replacing a general hierarchy level ν by a moment matrix with block-dependent levels ν_l. This allows to define hybrid levels where, for instance, smaller blocks are generated at higher values of ν_l, thus improving the quality of the lower bound without significantly affecting the scalability of the SDP.

Let us illustrate how this chordal extended relaxation works in practice, by going back to the three spins example introduced in the previous subsection. Imagine one wants to solve the 1D Ising model with Hamiltonian $H = \sum_{i=1}^{2} J_{i,i+1}\sigma_i\sigma_{i+1}$. The corresponding dependency graph G is already chordal and is composed of two cliques $C_1 = \sigma_1, \sigma_2$ and $C_2 = \sigma_2, \sigma_3$. Then, for a relaxation at level $\nu = 2$ the matrix (6.5) can be substituted by the two blocks:

$$\Gamma_{C_1}^{(2)} = \begin{pmatrix} 1 & \langle\sigma_1\rangle & \langle\sigma_2\rangle & \langle\sigma_1\sigma_2\rangle \\ \langle\sigma_1\rangle & 1 & \langle\sigma_1\sigma_2\rangle & \langle\sigma_2\rangle \\ \langle\sigma_2\rangle & \langle\sigma_1\sigma_2\rangle & 1 & \langle\sigma_1\rangle \\ \langle\sigma_1\sigma_2\rangle & \langle\sigma_2\rangle & \langle\sigma_1\rangle & 1 \end{pmatrix} \tag{6.7}$$

$$\Gamma_{C_2}^{(2)} = \begin{pmatrix} 1 & \langle\sigma_2\rangle & \langle\sigma_3\rangle & \langle\sigma_2\sigma_3\rangle \\ \langle\sigma_2\rangle & 1 & \langle\sigma_2\sigma_3\rangle & \langle\sigma_3\rangle \\ \langle\sigma_3\rangle & \langle\sigma_2\sigma_3\rangle & 1 & \langle\sigma_2\rangle \\ \langle\sigma_2\sigma_3\rangle & \langle\sigma_3\rangle & \langle\sigma_2\rangle & 1 \end{pmatrix} \tag{6.8}$$

The constraints $G_{l,n}$ derive from that the variable σ_2 belongs to both cliques, hence many expectation values appear in both blocks. Some of

the unnecessary expectation values in (6.5), such as $\langle\sigma_1\sigma_3\rangle$ and $\langle\sigma_1\sigma_2\sigma_3\rangle$ no longer appear in the two smaller blocks $\Gamma^{(2)}_{C_1}$ and $\Gamma^{(2)}_{C_2}$. Such a simplification is particularly useful because it reduces the number of variables involved in the SDP. Although the $G_{l,n}$ constraints do not allow to split the problem into n_C independent ones, one can still see that the scaling of the computational effort is dominated by the size of the largest block alone.

Branch and bound techniques to solve the ground state energy problem

The state-of-the-art techniques to compute exact solutions to the ground state problem rely on the BB method. This is a general iteration strategy that has been applied in several different ways (see, for instance, Ref. [RRW08] for a review). However, all different applications build upon three main ingredients:

1. *Lower bound*: a method to find a lower bound to the ground state energy. This generally implies the use of some relaxation of the ground state energy problem.

2. *Upper bound*: some heuristics that gets a spin configuration that constitutes an approximation from above to the ground state energy. A simple example would be classical annealing. As mentioned before, we use a procedure to extract a spin configuration directly from the solution of the SDP relaxation.

3. *Branching procedure*: a branching consist in dividing the original problem into two sub-problems that corresponds to the opposite cases of a dichotomic choice. In the ground state search, it can be done by choosing a vertex i and considering the two sub-sets of spin configurations that have $\sigma_i = \pm 1$ fixed. Solving the ground state problem in both of the sub-cases can be cast as another ground state problem for a modified graph where the vertex i has been removed and the couplings have been modified accordingly. Then, clearly, the solution of the original ground state energy is just the minimum between the solutions of the two sub-cases.

The trick is now to use the upper and lower bounds to reduce the number of branches to explore. The BB procedure does that as follows: (i) start with the original graph and compute a lower and upper bound z_L, z_U to the ground-state energy; (ii) if the bounds differ, choose a branching and compute lower and upper bounds for the two subcases; (iii) keep

track of the best upper bound $\bar{z}_U$ encountered so far and discard all the explored branches in which the lower bound is higher than $\bar{z}_U$; (iv) from the reduced list of branches, pick the one corresponding to the lowest z_L, if it still differs from the best upper bound $\bar{z}_U$, go back to point (ii) and perform another branching; (v) keep repeating until the lowest z_L and the best upper bound $\bar{z}_U$ coincide.

6.3.2 Details of the method

We now describe in detail the three ingredients of our chordal branch and bound (CBB) strategy: the lower bound, the upper bound, and the branching rule.

Lower bound

The cheapest method to get a bound on the ground-state energy from below would be to use the relaxation in (6.6) at its lowest level, namely $\nu = 1$. However, in practical applications this leads to a lower bound that can be more than 10 % away from the corresponding upper bound. As already mentioned in Ref. [RRW08], having such a big initial gap slows down the convergence of the branch and bound, making it very difficult to reach a point in the branching where the lower bound is high enough to start excluding the first branches. This problem is overcome by tightening the relaxation, which can be done in several ways.

The option considered in Ref. [RRW08] was to tighten the relaxation at level 1 by adding hand crafted linear inequalities, so-called triangle inequalities, between entries of the matrix corresponding to the two-body correlations $\langle \sigma_i \sigma_j \rangle$ of triples of spin variables. Since the amount of all these possible constraints scales as N^3, usually only part of them is introduced. In our CBB we can exploit the structure of the problem to obtain more systematic efficient improvements.

The chordal extension reduces the amount of meaningful constraints that can be added. Indeed, the resulting block structure implies that the only two-body expectation values $\langle \sigma_i \sigma_j \rangle$ that appear in the moment matrices correspond to spins i, j belonging to the same block. Hence, all the triangle inequalities that can actually be imposed have to involve triples i, j, k that appear in the same clique.

The numerical effort for one step in the CBB method is mostly determined by the largest block in the moment matrix. Therefore, we choose to take a hybrid approach, introducing an intermediate level with $\nu = 2$ for all the blocks $\Gamma_l^{(\nu)}$ involving less than n_t variables, while keeping all the bigger blocks at level 1. Taking such a hybrid level yields a significant

improvement in the initial lower-upper bound gap already for smaller values of n_t. In fact, we have checked numerically that this devises a test that corresponds at least to the case of level 1 plus the addition of all triangle inequalities between variables in the smaller blocks.

Moreover, we also allow for additional triangle constraints between two-body correlations belonging to bigger blocks. In particular, we add them in an iterative way, as shown in Ref. [RRW08], until the improvement on the lower bound is smaller than some numerical precision. In most cases we tested, there was actually no need to introduce these additional constraints.

Upper bound

For the upper bound one needs a good guess for a spin configuration that is close to the ground-state energy. Here we develop an improvement over the method proposed in Ref. [RRW08]. A nice feature of the method is that it extracts an upper bound directly from the moment matrix that is obtained by solving the SDP to get the lower bound. Intuitively, this can be seen as a way to obtain the spin configurations "closest" to the optimal (but typically unphysical) solution achieved by the relaxation.

Recall from Section 6.3.1 that the method we use has a very simple interpretation: take the moment matrices $\Gamma_l^{*(\nu)}$, obtained from the solution of the SDP (6.6), and construct the configuration $\vec{\sigma}^*$ where each spin σ_i^* is aligned according to the sign of the entry corresponding to the expectation value $\langle\sigma_i\rangle$. For the sake of comparison with Ref. [RRW08], let us explain its interpretation in more detail: recall that each matrix $\Gamma_l^{*(\nu)}$ always contains as a sub-matrix $\Gamma_l^{*(1)}$, involving the variables occurring already at level 1, namely that generated by the set of variables $\{1, C_l\}$. $\Gamma_l^{*(1)}$ is a $(n_l+1)\times(n_l+1)$ matrix, where n_l stands form the number of spins contained in the clique C_l (compare also the examples in Eqs. (6.7) and (6.8)).

Because they are positive semidefinite, these matrices can be identified with a collection of vectors $\{v_{l,0}, v_{l,1}, \ldots, v_{l,n_l}\}$ in a $m-$dimensional space $\mathbb{R}^m$ that reproduce their entries by the scalar product $\Gamma_{l,ij}^{*(1)} = v_{l,i}\cdot v_{l,j}$. A way to obtain such vectors is to perform a Cholesky decomposition of the moment matrices $\Gamma_l^{*(1)} = B_l^T B_l$ and reduce the columns of the resulting B_l up to the point where $\Gamma_l^{*(1)}$ can still be recovered to the desired numerical precision.

Inspired by a similar argument used in Ref. [NPA08], we interpret the first vector $v_{l,0}$ of each block as a representation of a state of the spin systems, while the remaining vectors represent the spin variables in the

clique C_l. Indeed, one can see that the first row of the moment matrices recovers the spin expectation values $\Gamma^{*(1)}_{l,0j} = v_{l,0} \cdot v_{l,j} = \langle \sigma_j \rangle$. Now we can define a spin configuration for the clique C_l from the sign of these scalar products, i.e., we set the variables of the jth spin in the lth subset to be $\text{sign}(v_{l,0} \cdot v_{l,j})$.

This method is different from what had been done in earlier approaches. In Ref.
[RRW08], the moment matrix is missing the first row and column vector, and thus exactly the entries we need. In this case, a configuration had to be extracted via the $\text{sign}(v_r \cdot v_{l,j})$ of inner products between $v_{l,j}$ and randomly chosen vectors v_r. Constructing spin configurations via random vectors in this way is incompatible with the chordal extension, let us explain why: since the cliques of a graph overlap on some vertices, it will happen that the same spin index appears in more than one list I^l. However, given that the aim is to extract a complete and consistent spin configuration $\vec{\sigma}^* = \{\sigma_1^*, \ldots, \sigma_n^*\}$, one must avoid having conflicting assignments for any of the spin variables. If one takes the randomised construction from Ref. [RRW08], such inconsistencies will appear, even if the random vectors v_r are taken to be the same for each block. On the contrary, since we essentially set each deterministic guess to be the sign of a one-body expectation values, our method ensures consistency.

To conclude, once a valid spin configuration $\vec{\sigma}^*$ has been extracted, we simply set the upper bound to be its corresponding energy $H(\vec{\sigma}^*)$. Surprisingly, we noticed that by following this procedure, the exact ground states is usually recovered very soon in the branching (see Fig. 6.1 for an example). It then takes additional time to find a matching lower bound to verify that this is indeed the lowest achievable energy. This makes us believe that the outlined procedure is very efficient in finding the optimal deterministic configuration.

Branching rule

Here we follow the same method outlined in [RRW08], but with a different choice of branching procedure. Indeed, the authors in [RRW08] choose the dichotomic choice to be the relative alignment of a pair of connected spins. That is, given a choice of indices i, j, the two branches correspond to the two cases $\sigma_i \pm \sigma_j = 0$. However, as mentioned before, we prefer to branch on the value of the single spin, by choosing between the two values $\sigma_i = \pm 1$. The reason for this is that, in the latter case the number of possible branching steps depends only on the number N of spins in the system. On the contrary, the former method involves an amount of branching choices that depends on the number of edges in the dependency

graph G, which can be much higher, often as high as N^2.

Finally there is the question of which spin i to choose for the next branching. The way we do this here, is based on the corresponding expectation value $\langle\sigma_i\rangle$ recovered from the moment matrices $\Gamma_l^{(\nu)}$ obtained by solving the SDP. The intuition is the following: spins with an expectation value close to zero are "difficult" choices, because flipping the value of such a spin is likely to lead to a slight change in the energy of the system; conversely, expectation values very close to ± 1 are identified as "easy" choices, because flip such a spin is likely to lead to a significant change in the energy of the system. We set the branching rule to "easy-first", that is, at the end of each optimisation round, the next branching is performed on the most deterministic spin in the $\Gamma_l^{(\nu)}$.

6.4 Benchmarking the CBB

We now describe the results that we could obtain by benchmarking the CBB method with other classical and quantum algorithms. We start with a comparison of the standard SDP-based BB methods and CBB and then move on to the more interesting problem of verifying the results of two kinds of energy minimisations performed on an actual quantum annealing device. To do so, we also show how the results obtained by CBB can be used to study the phase transition in a 2D triangular ferromagnetic Ising model with local disorder. The numerical minimisation with CBB and BB was run on a workstation with an Intel Xeon E5-1650v4 processor with six physical cores clocked at 3.60 GHz base frequency and 128 GByte RAM. Due to the polynomial scaling of the method, much larger system sizes can be reached with more powerful hardware. The sparse semidefinite relaxations were generated by Ncpol2sdpa [Wit15], and the semidefinite programs were solved by Mosek [Mos]. The code for the experiments is available under an open source license [1].

6.4.1 Ising model on a 2D square lattice

As a first test we compare the performance of the CBB method with a sparse Ising problem in the two cases of exploiting and not exploiting the chordal extension trick. In the absence of chordal extension, our BB method is comparable to the one introduced in [RRW08] (for details, see Section 6.3). As a benchmark of a sparse instance, we consider the standard 2D ferromagnetic Ising model in a statically disordered magnetic field (quenched disorder). Such a model is represented by the following

[1] `https://gitlab.com/FBaccari/Chordal_BB`

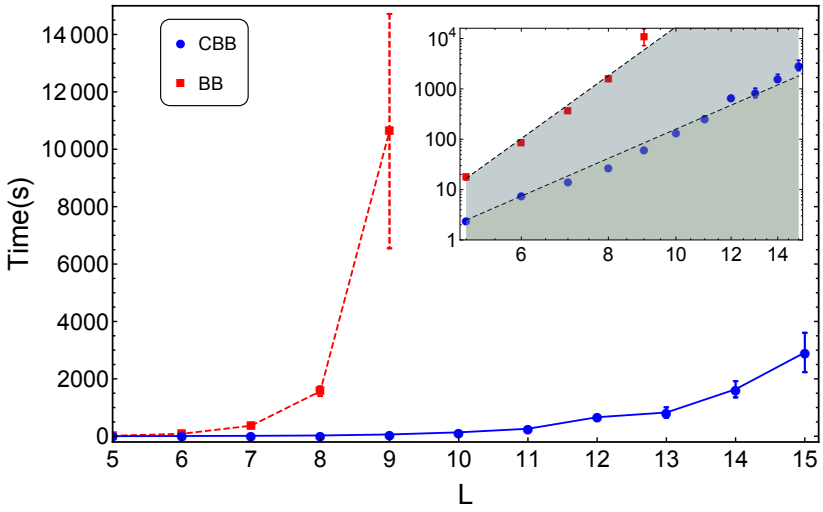

Figure 6.3: Time comparison, as a function of the linear lattice size $L = \sqrt{N}$, between a standard SDP-based branch and bound (BB) algorithm and the one augmented with the chordal extension (CBB). The problem is finding the ground state energy for a 2D Ising ferromagnetic model with random Gaussian magnetic field, close to the phase transition at $\sigma = 1.5$, i.e. where the ground state is already partially disordered. The time estimation was averaged over 100 disorder realisations, except for the largest system size, where the averaging was reduced to 10 samples. Due to the large amount of disorder averaging, we limit ourselves to system sizes $L \leq 15$, far below the maximum sizes we can tackle on our hardware. The comparison is shown in a linear scale and double logarithmic in the inset. The dashed lines in the inset are power laws of the form L^{10} and L^6, demonstrating the claimed polynomial scaling of the runtime N^5 for BB vs. N^3 for CBB.

Hamiltonian

$$H(\vec{\sigma}) = -\sum_{\langle i,j \rangle} \sigma_i \sigma_j + \sum_{i=1}^{N} h_i \sigma_i \,, \tag{6.9}$$

where the first sum runs over all pairs of connected spins $\langle i, j \rangle$ in a square lattice. The local fields h_i are drawn randomly from a Gaussian distribution with zero mean and variance σ for each site i. As a function of the disorder strength σ, the model undergoes a phase transition from a ferromagnetic ground state (in which all states are aligned with each other) to a disordered phase (in which, for extremely large disorder, the spins are aligned with the local magnetic fields). For this model it is known

that the ground state can in principle be found in polynomial time (for details see Section 6.2.2).

Indeed, the non-chordal BB method is able to do that, but, especially in the interesting region close to the phase transition, fast growing memory requirements and runtime make the method impractical for systems that are larger than 15×15 on the hardware we have at our disposal. The CBB method, in contrast, allows us to solve systems of over 35×35 sites on the same hardware, due to both lower memory requirements and a very significantly reduced runtime, both in terms of absolute numbers and in terms of scaling (see Figure 6.3 for a comparison). While the runtime of non-chordal BB exhibits a roughly N^5 dependence on the number of spins N, CBB scales roughly as N^3.

6.4.2 Verifying the solution of a D-Wave quantum annealer

We now turn to the verification of a ground state energy search by quantum annealing. To show the flexibility of the CBB method and also to verify a quantum annealing solution for the largest system size simulable on a state-of-the-art annealer, we move to a more interesting and slightly less spares lattice, namely the 2D triangular lattice. Spin models on the triangular lattices display a wealth of interesting physical phenomena, many driven by the possibility to have frustrated interactions. To remain in a regime that is comparable to the benchmarking we did before, we however concentrate on the interplay of ferromagnetic interactions with a disordered magnetic field.

We used a D-Wave 2000Q quantum annealer with 2040 functional qubits. The chip had 8 faulty qubits and the corresponding couplings were removed from a full-yield 16×16 Chimera graph. We used the virtual full-yield Chimera graph abstraction to ensure consistent embeddings and improve the quality of the results. The coupling strengths were automatically scaled to the interval $[-1, 1]$, and the logical qubits used a coupling strength of -2 to hold a chain of physical spins together. The minor embedding was a heuristic method, yielding a chain length of 7. We also tried chains up to length 22, without significant change in the results, showing that the scaling in the couplings ensures that the chains do not break. For each data point, we sampled a thousand data points and chose the one with the lowest energy as the optimum. This takes constant time irrespective of the values set, in the range of milliseconds. The flux bias of the qubits was not offset.

Both the quantum annealer and the CBB simulation were done for the same disorder realisations (the disorder in the annealer is fully pro-

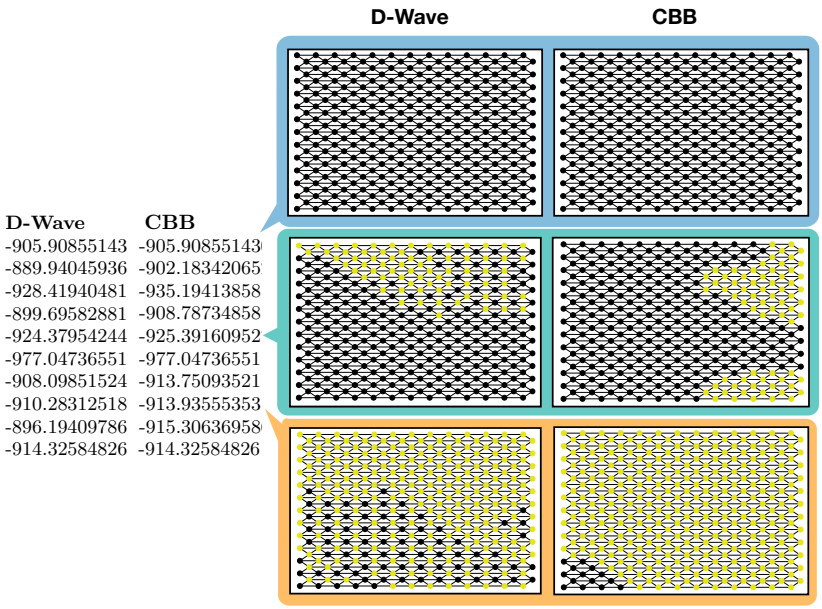

Figure 6.4: Left: Comparison of the lowest energy value for a disordered phase at $\sigma = 1.5$ on a triangular lattice on a 2040-qubit quantum annealer and the chordal branch and bound algorithm. Right: comparison of the corresponding ground state spin configuration for the case where the lowest energy was not achieved. Yellow spins are $+1$ and black one -1. It can be seen clearly that, even when the two energies are close, the corresponding spin configurations can be very different. This shows that the excited state that the D-Wave quantum annealer returns, does not necessarily resemble the globally optimal solution.

grammable) to obtain directly comparable results. We observe that for most disorder realisations, we can verify by CBB that the quantum annealer is able to find the exact ground state energy. This is true even for intermediate disorder strength, where the ground state spin pattern shows macroscopic islands of aligned spins whose precise shape and positions depends non-trivially on the disorder realisation around $\sigma = 1.5$. It does that typically in a very short time. However, there are also cases in which, even after 1000 repetitions, the lowest energy found by the quantum annealer is still higher than the exact value computed with CBB. Here, the optimal spin configuration found by the quantum annealer typically differs markedly from the true ground state, which shows that it gets stuck in local minima and emphasises the importance for exact methods such as CBB for comparison and benchmarking. We summarise results

of simulations in this interesting regime of intermediate disorder strength in Figure 6.4.

6.4.3 Analysis of the phase transition in the ferromagnetic disordered Ising model in a 2D triangular lattice

Here we use the CBB method to study in more detail the 2D triangular Ising model used to benchmark the solution of the D-wave quantum annealer. Recall that we considered a ferromagnetic model in a statically disordered magnetic field, represented by Hamiltonian (6.9), where now the first sum runs over all pairs of connected spins $\langle i, j \rangle$ in the triangular lattice. The phase transition can be detected by estimating the ground state magnetisation

$$m = \frac{|\sum_{i=1}^{N} \sigma_i^{(g)}|}{N}\,, \tag{6.10}$$

where $\vec{\sigma}^{(g)}$ is the ground state configuration. Clearly, a ferromagnetic ground states is fully magnetised, hence it is characterised by $m = 1$. On the other hand, a disordered phase corresponds to $m \approx 0$ (notice that, because of finite size effects, one can never reach an exactly zero value in numerical tests).

We analysed the phase transition by computing the ground state energy for the model with the CBB method and estimating its magnetisation m as a function of the disorder strength σ. For each value of σ, the results were averaged over 100 samples. Figure 6.5 shows the obtained magnetisation curves, for two different linear lattice sizes $L = 15, 20$.

6.4.4 Verifying solutions for a Chimera graph

Lastly, we consider the application of CBB to a denser graph. For this purpose we choose the Chimera architecture [BHJ$^+$14], which is the natural graph on the D-wave 2000Q hardware. The corresponding graph is composed of $K_{4,4}$ fully connected bipartite unit cells, consisting of 8 spins – 4 horizontal and 4 vertical – with edges between each horizontal/vertical pair. These unit cells are arranged to form a 2D square lattice of size L and a total number of $N = 8\,L^2$ spins. Because of the in-cell connectivity, such a graph is clearly non-planar and thus has the potential to encode NP-hard Ising models. We consider again a ferromagnetic model with a disordered magnetic field and we find that even though the Chimera graph is non-planar and denser than 2D rectangular and triangular lattice, using the chordal extension still gives a remarkable advantage, allowing us to compute the ground state energy for system

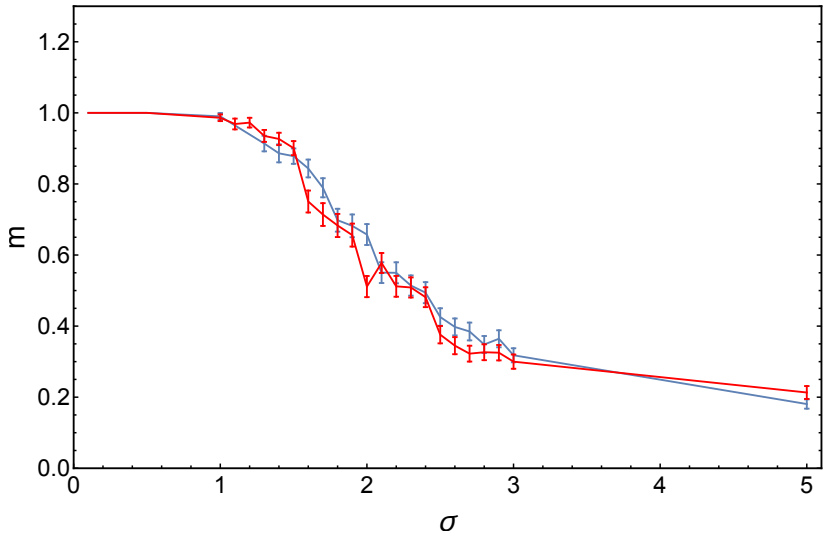

Figure 6.5: Average magnetisation m of the ground state of the ferromagnetic Ising model with disordered magnetic field, as a function of the disorder strength σ, for a 2D triangular lattice of linear size L. The plot shows the cases $L = 15$ (blue) and $L = 20$ (red). The phase transition could be pinned-down more precisely by means of a finite size scaling analysis. For our purposes here it is sufficient to know that in the range $\sigma \in [1, 3]$, the ground states has non-trivial spin patterns.

sizes of $L = 9$, compared to just $L = 5$ (on the same hardware) for an SDP-based BB method without the chordal extension.

Let us stress that, although the D-Wave 2000Q quantum annealer is currently implementing a Chimera graph with 2040 functional physical qubits, they are seldom actually used as logical spins. Most recent studies encode each $K_{4,4}$ cell as a single logical spin, in order to suppress errors due to the finite size and qubit quality of the system [MK18]. This results in effectively solving Ising models on a 2D square lattice which, being planar, is actually proven to be polynomially solvable (see also Section 6.2.2). On the contrary, our numerical test was performed on the actual Chimera graph. This opens up the way to benchmarking future annealing devices, once their physical qubit quality has improved to a point that makes the individual spins useful, in the much more interesting regime of non-planar graphs.

6.5 Discussion and possible improvements

Designing methods to certify the output of quantum optimisers is crucial for their development. In this Chapter we introduced the chordal branch-and-bound (CBB) method that uses a hierarchy of efficiently computable upper and lower bounds on the ground-state energy of classical spin systems and exploits the physical locality structure of relevant Hamiltonians. Our numerical results show that the iterative branch-and-bound process often converges, providing an exact and certified value for the ground-state energy, together with a ground-state configuration. The favourable scaling in memory and runtime of our method, compared to methods that do not use the chordal extension, enables the verification of current and near-future quantum optimisers, such as the D-Wave quantum annealer [LPS+14], degenerate optical parametric oscillators [QNN17], and variational circuits [FGG14, Cro18].

Notice that there is some extent of freedom in the way we implemented our CBB method. Given the huge difference in complexity that can be exhibited by various instances of the Ising model, we expect the optimal choice to be model dependent. Let us briefly discuss which modifications we imagine to be most useful for practical applications.

We start by recalling that, in order to accelerate the convergence process and to keep memory requirements low, it is crucial to reduce the initial lower-upper bound gap as much as possible and as early as possible. One way to do that is to modify the hybrid hierarchy level introduced above. In our applications, it was always enough to set the threshold to at most $n_t = 7$. However, such value can be significantly increased without affecting too much the scalability of the CBB. Indeed, the main bottleneck of our method is the memory required to solve the largest SDP. This depends mainly on the block l^* leading to the largest matrix $\Gamma^{(\nu)}_{l^*}$. Therefore, as long as increasing the level of the smaller blocks does not lead to bigger matrices that the one for the largest clique, the SDP will still have the same memory requirements – although the solving time will clearly increase.

Other branching rules can be also be adopted. For instance, one can replace the "easy-first" approach with a "difficult-first". In this case, one picks the next branching from the least deterministic spin in the $\Gamma^{(\nu)}_{l}$ We expect the choice of the most effective branching rule to depend on the system under consideration.

Lastly, there are instances in which CBB does not outperform other methods. This is true for specific cases of very sparse problems, where linear-programming relaxations were shown to work very well [LJRR04], or some hand-crafted models for which exact polynomial algorithms are

known [MKT17]. Nevertheless, it would still be interesting to see if one could combine the construction based on the chordal extension with those methods and provide some further advantage.

Chapter 7

Conclusions and outlook

Certifying operational properties of many-body systems is a crucial problem for the development of quantum technologies. Importantly, any certification protocol that aims at applying to large scale scenarios has to fulfil scalability requirements that are two-fold. From the computational point of view, it has to be based on a numerical test whose memory and time requirements are polynomial in the number of particles in the state. Similarly, it must require an amount of information that can be estimated experimentally with a polynomial effort too.

The device-independent framework, based on the detection of nonlocality, a property that can be assessed by simply looking at correlations, is particularly appealing for certifying purposes. Indeed, it provides methods to characterise properties of a quantum device without having to know the details of its internal functioning. In this thesis, we studied scalable device-independent methods for the certification of several operational features of multipartite systems. Moreover, we extended techniques we developed for nonlocality detection so to address a completely different framework, namely that of computing the ground state energy of a classical spin system.

In this Chapter we briefly revise the scenarios and applications we considered and discuss possible future lines of investigation for each of them.

Device-independent detection of entanglement. We have studied a relaxation of the nonlocality detection problems in terms of an SDP. Such a relaxation allows one to define a numerical device-independent test for entanglement in a multipartite system that is scalable both from the computational and the experimental point of view. Indeed, the related SDP involves a polynomial amount of variables in the size of the system

and it requires the knowledge of few-body correlations only. We have also shown that the propose method, despite being a relaxation, successfully detects entanglement in several physically relevant families of multipartite states.

An interesting question to address would be whether the SDP test can be used to provide also quantitative statements about the entanglement in the system. This would require to study relaxations of the nonlocality depth detection problem, which would give information on how many particles in the system are really entangled among each other.

Alternatively, it would also be relevant to analyse the proposed method in more detail. Notice, for instance, that if one is interested in knowing whether a given state is entangled, one has to generate correlations to feed the SDP. This requires making a specific choice of local measurements to perform and it clearly affects the results of the test: in other words, depending on which measurements one considers, the same entangled state might be detected or not by the SDP condition. Therefore, if we aim at applying our method to realistic scenarios, studying good strategies to generate correlations that allow for successful entanglement detection is of vital interest.

Lastly, it would be worth exploring the possibility of applying the introduced entanglement detection techniques to real data coming from an experiment.

Detecting nonlocality depth in many-body systems. We have studied the problem of detecting nonlocality depth in many-body systems, namely quantifying how many particles genuinely share nonlocal correlations, with the limited knowledge of two-body correlators. We have shown that, upon considering permutationally invariant correlations, the problem drastically simplifies: more precisely, any fixed nonlocality depth can be detected with a test that is polynomial in the number of particles. Moreover, we have introduced a Bell inequality that can discriminate values of nonlocality depth of $k \leq 6$ for systems of any size and we have applied it to experimental data from a Bose-Einstein condensate composed of several hundreds of particles.

Given these results, a natural question that comes in mind is whether two-body correlations are enough to detect any value of nonlocality depth, including genuine nonlocal correlations. While we know that this is the case for systems of up to $N = 7$ particles, the problem is still open in the case of arbitrarily large systems. To answer such question one should know the projection of the no-signaling polytope in the two-body symmetric space for scenarios of any number of particles, a problem we

conjecture being too hard to be solved in general. Nevertheless, it would be interesting to see whether considering relaxations of the problem could be of any help.

On the other hand, it would also be of interest to classify families of multipartite states whose nonlocality depth can be detected in the considered two-body framework. We know from previous works that spin-squeezed states and Dicke states are good candidates for standard nonlocality detection, but inequalities that discriminate values of nonlocality depth for Dicke states of any number of particles are yet to be found.

Scalable self-testing based on Bell inequalities. We have introduced a general strategy to derive self-testing Bell inequalities maximally violated by graph states, one of the most paradigmatic families of multipartite states. We have also shown that the violation of these inequalities can be used to bound the fidelity between the measured state and the graph state of interest. Compared to previously known inequalities for graph states, ours are the first to be associated to a self-testing statement and they are also the most scalable ones, since they are composed of a number of terms that scales linearly with the system size.

From an experimental point of view, the introduced Bell inequalities constitute a promising certification tool that can be readily used in any setup that is currently generating graph states. Thus, it would be interesting to explore this possibility, which would be the first application of device-independent fidelity bounds to experimental data. The main obstacle to face is that, for the current bounds to be meaningful, the state has to be produced with a very high fidelity (about $90 - 95\%$), which is a very strict requirement for the state-of-the-art methods to generate graph states. A way to cope with this problem would be to look for device-independent bounds for our Bell inequalities that are more resilient to experimental imperfections.

From a more theoretical point of view, it would also be interesting to explore generalisations of our method to self-test other classes of multipartite states. Indeed, as we have shown with the example of the partially entangled GHZ state, one can interpret our techniques as a way to derive inequalities associated to the stabilizers of a generic multipartite state. The range of applicability of such techniques is yet a very open question. Apart from self-testing of states and measurements, a promising direction to investigate is the extension of our method to the device-independent certification of other quantum information protocols. Two promising examples we can think of are quantum computing and quan-

tum error correction. In fact, a representative model of universal quantum computation is constituted by measurement-based quantum computing [RB01], whose building block is the cluster state, precisely a graph state. Similarly, many quantum error correction protocols can be interpreted by means of a stabilizer formalism. Hence, both the outlined scenarios present connections to our method that might be worth exploring further.

Verification of Quantum Optimizers. We have introduced the chordal branch-and-bound method, a scalable numerical tool to compute a convergent series of upper and lower bounds to the ground state energy of any classical spin model. Even though the complexity of the problem implies that for some models the convergence will be met in exponential time, CBB is guaranteed to output with polynomial effort a confidence region enclosing the exact solution.

Our method constitutes a very promising tool to verify the solutions provided by newly developed quantum optimizers. We have already shown an application to the D-Wave quantum annealer, which allowed us to detect instances where the device got stuck in a local minimum. On a related note, it would be interesting to study whether CBB could be used to certify the quality of a given quantum optimisation method. For instance, one could use our method to check whether a quantum device reaches the exact solution for small system sizes and then leave the large instances to the quantum algorithm only, while checking the validity of the output through the confidence region that CBB provides in an efficient way.

A direction worth exploring is also a further comparison to other branch-and-bound methods, especially those based on linear programming, that have been shown to be very scalable for some specific examples of sparse Ising models. In particular, it would be interesting to see whether the techniques involved in CBB can be combined with insights coming from these methods, in order to obtain even more efficient certification algorithms for the classical ground state energy problem.

Lastly, it would be very interesting to study whether a method similar to CBB can be used to derive a convergent series of lower and upper and bounds to the ground state energy of quantum Ising models.

Appendix A

Appendix of Chapter 3

A.1 Details of the method

Here, we present in more detail the SDP relaxation associated to quantum realisations with commuting measurements. In order to be consistent with the examples presented in the main text, we express it in terms of correlators, but we stress that a formulation in terms of projector and probabilities for higher numbers of outcomes is straightforward.

Let us consider that the N observers A_i are allowed to perform m dichotomic measurements each. We can therefore define the expectation value operators $M_{x_i}^{(i)} = M_{x_i}^1 - M_{x_i}^0$ in terms of measurements $M_{x_i}^{a_i}$, so to reproduce the correlators (3.4).

For any quantum realisation of such operators, it is possible to show that they satisfy the following properties:

i) $(M_{x_i}^{(i)})^\dagger = M_{x_i}^{(i)}$ for any $i = 1, \ldots N$ and $x_i = 1, \ldots, m$,

ii) $(M_{x_i}^{(i)})^2 = \mathbb{1}$ for any $i = 1, \ldots N$ and $x_i = 1, \ldots, m$,

iii) $[M_{x_i}^{(i)}, M_{x_j}^{(j)}] = 0$ for any $i \neq j$ and $x_i, x_j = 1, \ldots, m$.

Now, let us consider that the sets $\mathcal{O}_\nu$ we introduce in section 3.2.1 consist exactly of all the products of the $\{M_{x_i}^{(i)}\}$ up to order ν. Then, by indexing the operators in the sets as $\mathcal{O}_i$ for $i = 1, \ldots, k$, we define the $k \times k$ moment matrix as follows

$$\Gamma_{ij} = tr(\rho_N \mathcal{O}_i^\dagger \mathcal{O}_j)$$

where ρ_N is a generic N-partite quantum state. As it was shown in [NPA07, NPA08], for any set of quantum correlations P, the properties

i)-iii) and the fact that the associated ρ_N is a proper quantum state reflect into the following properties of the moment matrix:

- $\Gamma^\dagger = \Gamma$,
- $\Gamma \succeq 0$,
- the entries of the matrix are constrained by some linear equations of the form

$$\sum_{i,j} (F_m)_{ij} \Gamma_{ij} = g_m(P) \quad m = 1, \ldots, l$$

where $(F_m)_{ij}$ are some coefficients and the $g_m(P)$ can depend on the values of the correlators composing the P vector, as such

$$g_m(P) = (g_m)_0 + \sum_{k=1}^{N} \sum_{\substack{i_1 < \ldots < i_k \\ i_1, \ldots, i_j}} (g_m)^{i_1,\ldots,i_k}_{j_1,\ldots j_k} \langle M^{(i_1)}_{j_1} \ldots M^{(i_k)}_{j_k} \rangle$$

Up to this point, the method we describe coincides with the NPA hierarchy [NPA07, NPA08], which is used to check whether a set of observed correlations is compatible with a quantum realisation. In order to define a hierarchy to test for local hidden variables realisation, we introduce the additional condition that all the measurements for the same party have to also be commuting, namely

iv) $[M^{(i)}_{x_i}, M^{(i)}_{y_i}] = 0$ for any $i = 1, \ldots, N$ and $x_i \neq y_i = 1, \ldots, m$.

It can be seen that property iv) implies a second set of linear constraints on the Γ matrix, which we identify as

$$\sum_{i,j} (F'_m)_{ij} \Gamma_{ij} = g'_m(P) \quad m = 1, \ldots, l'$$

To make it clearer, we show an example of linear constraint that can come only if we impose condition iv). Let us consider the following four operators: $\mathcal{O}_k = M^{(i)}_{x_i} M^{(i)}_{y_i}$, $\mathcal{O}_l = M^{(i)}_{x_i} M^{(j)}_{x_j}$, $\mathcal{O}_n = M^{(i)}_{y_i}$ and $\mathcal{O}_m = M^{(j)}_{x_j}$. It is easy to see that, by exploiting i)-iii) plus iv), $\Gamma_{kl} = \Gamma_{nm}$ for any choice of $x_i, y_i, x_j = 1, \ldots, m$ and $i, j = 1, \ldots, N$.

Now, for any chosen $\mathcal{O}_\nu$, we can test whether an observed distribution P is compatible with a local model via the following SDP

$$\begin{aligned} &\text{maximise} \quad \lambda, \\ &\text{subject to} \quad \Gamma - \lambda \mathbb{1} \succeq 0, \\ &\qquad \sum_{i,j} (F_m)_{ij} \Gamma_{ij} = g_m(P) \quad m = 1, \ldots, l \ , \\ &\qquad \sum_{i,j} (F'_m)_{ij} \Gamma_{ij} = g'_m(P) \quad m = 1, \ldots, l' \ , \end{aligned} \tag{A.1}$$

which is the *primal form* of the problem. A solution $\lambda^*_{min} < 0$ implies that it is not possible to find a semidefinite positive moment matrix satisfying the given linear constraints. Therefore P has no quantum realisation with commuting measurements and we conclude it is nonlocal. We notice that by increasing the value of ν we get a sequence of more and more stringent tests for nonlocality. Indeed, the linear constraints for the level ν are always a subset of the ones coming from $\nu + 1$. Moreover, in analogy with the NPA hierarchy, the series of tests is convergent; hence any nonlocal correlation will give a negative solution λ^*_{min} at a finite step of the sequence.

Interestingly, we can also study the *dual form* of the SDP problem, which reads as follows:

$$\begin{aligned} &\text{minimise} \quad G(P) = \sum_k y_k g_k(P) + \sum_k y'_k g'_k(P), \\ &\text{subject to} \quad \sum_k y_k F_k^T + \sum_k y'_k F'^T_k \succeq 0, \\ &\qquad \sum_k y_k \mathrm{tr}(F_k^T) + \sum_k y'_k \mathrm{tr}(F'^T_k) = 1. \end{aligned} \tag{A.2}$$

Thanks to the strong duality of the problem, a negative solution for the primal implies also $G(P) = \lambda^*_{min} < 0$. Since any point in $\mathcal{L}_\nu$ satisfies the SDP condition at level ν with $G(P) \geq 0$, we can interpret $G(P)$ as a Bell-like inequality separating the $\mathcal{L}_\nu$ from the rest of the correlations. Indeed, since $g_k(P)$ and $g'_k(P)$ are linear in terms of the probability distribution, we derive that $G(P) \geq 0$ defines also a linear inequality for P. Violation of such an inequality directly implies nonlocality.

A.2 Proof of local bound and quantum violation for the inequalities

We start by proving the local bounds for the inequalities introduced in the main text. To do so, we remind the reader that to derive the

maximal value attained by local correlations it is enough to maximise over the vertices of the local set. In the correlator space, the deterministic local strategies (DLS) take the form

$$\langle M_{j_1}^{(i_1)} \ldots M_{j_k}^{(i_k)} \rangle = \langle M_{j_1}^{(i_1)} \rangle \ldots \langle M_{j_k}^{(i_k)} \rangle \tag{A.3}$$

where each $M_{x_i}^{(i)}$ term can take only 1 and -1 values. By using this property, inequality (3.10) becomes

$$\begin{aligned} \mathcal{I}_{mix}^{3}(DLS) = (N-1) \left[\langle M_1^{(1)} \rangle + \langle M_0^{(1)} \rangle \right] \mathcal{T}_0 \\ + \left[\langle M_1^{(1)} \rangle - \langle M_0^{(1)} \rangle \right] \mathcal{T}_2 \end{aligned} \tag{A.4}$$

where $\mathcal{T}_0 = \langle M_0^{(2)} \rangle \ldots \langle M_0^{(N)} \rangle$ and $\mathcal{T}_2 = \sum_{i=2}^{N} \langle M_2^{(i)} \rangle$. For any number of parties N, we have that $\mathcal{T}_0 \leq 1$ and $\mathcal{T}_2 \leq N-1$; therefore

$$\mathcal{I}_{mix}^{3}(DLS) \leq 2(N-1) \langle M_1^{(1)} \rangle \leq 2(N-1) \tag{A.5}$$

Similarly, for any deterministic strategy, inequality (3.11) takes the from

$$\begin{aligned} \mathcal{I}_{mix}^{2}(DLS) = (N-1) \left[\langle M_1^{(1)} \rangle + \langle M_0^{(1)} \rangle \right] \mathcal{T}_0 \\ + \left[\langle M_1^{(1)} \rangle - \langle M_0^{(1)} \rangle \right] \mathcal{T}_1 \end{aligned} \tag{A.6}$$

where $\mathcal{T}_1 = \sum_{i=2}^{N} \langle M_1^{(i)} \rangle$. As for before, we can use the argument that $\mathcal{T}_0 \leq 1$ and $\mathcal{T}_1 \leq N-1$ to conclude

$$\mathcal{I}_{mix}^{2}(DLS) \leq 2(N-1) \langle M_1^{(1)} \rangle \leq 2(N-1) \tag{A.7}$$

Regarding the quantum violation, we recall that the scenario we consider is $|\psi\rangle = |GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$ with measurements choices $M_0^{(i)} = X$, $M_1^{(i)} = D = \frac{1}{\sqrt{2}}(X+Z)$ and $M_2^{(i)} = Z$ for all $i = 1, \ldots, N$. It is easy to check that, for a GHZ state of any number of parties, the following is true

- $\langle X_i X_j \rangle = \langle X_i Z_j \rangle = 0$ for any $i \neq j = 1, \ldots, N$.
- $\langle Z_i Z_j \rangle = 1$ and therefore $\langle D_i Z_j \rangle = \frac{1}{\sqrt{2}}$ and $\langle D_i D_j \rangle = \frac{1}{2}$for any $i \neq j = 1, \ldots, N$.
- $\langle X_1 X_2 \ldots X_N \rangle = 1$ and $\langle Z_1 X_2 \ldots X_N \rangle = 0$, therefore $\langle D_1 X_2 \ldots X_N \rangle = \frac{1}{\sqrt{2}}$ for any N.

By using the properties listed above, one can check that

$$\langle \mathcal{I}^3_{mix} \rangle_{GHZ_N} = (1+\sqrt{2})(N-1) \approx 2.41(N-1) \tag{A.8}$$

and, similarly, that

$$\langle \mathcal{I}^2_{mix} \rangle_{GHZ_N} = \frac{3+\sqrt{2}}{2}(N-1) \approx 2.21(N-1) \tag{A.9}$$

Moreover, we notice that by changing the measurement setting, one can achieve a higher violation of $\mathcal{I}^2_{mix}$. Indeed, it is easy to see that by choosing $M^{(1)}_0 = \frac{1}{\sqrt{2}}(X+Z)$, $M^{(1)}_1 = \frac{1}{\sqrt{2}}(X-Z)$ and $M^{(i)}_0 = X$,$M^{(i)}_1 = Z$ for $i = 2, \ldots, N$, the resulting violation is

$$\langle \mathcal{I}^2_{mix} \rangle_{GHZ_N} = 2\sqrt{2}(N-1) \approx 2.83(N-1) \tag{A.10}$$

To conclude, we proceed with the analysis of the robustness to noise. We recall that this implies considering the noisy version of the GHZ state; namely

$$\rho_N(p) = (1-p)\rho_{GHZ_N} + p\frac{\mathbb{1}_N}{2^N} \tag{A.11}$$

where $0 \leq p \leq 1$ represent the amount of white noise added to the state. It can be easily seen that the noise affects the values of the correlators for the GHZ state in the following way

$$\langle \sigma^{(i_1)} \ldots \sigma^{(i_k)} \rangle_{\rho_N} = (1-p)\langle \sigma^{(i_1)} \ldots \sigma^{(i_k)} \rangle_{GHZ_N} \tag{A.12}$$

for any $\sigma \in \{X, Y, Z\}$ and $1 \leq k \leq N$. Therefore we can consider the noise as a simple damping factor in the violation of the inequalities. By using this fact, we get that $\mathcal{I}^3_{mix}$ is violated as long as $(1-p)(1+\sqrt{2})(N-1) > 2(N-1)$; hence

$$p_{max}(\mathcal{I}^3_{mix}) = \frac{\sqrt{2}-1}{\sqrt{2}+1} \approx 0.17 \tag{A.13}$$

By the same argument, we analyse $\mathcal{I}^2_{mix}$ for the two measurements settings that we introduce. For the first one, the inequality is violated as long as $(1-p)\frac{3+\sqrt{2}}{2}(N-1) > 2(N-1)$ and, therefore,

$$p_{max}(\mathcal{I}^2_{mix}) = \frac{\sqrt{2}-1}{\sqrt{2}+3} \approx 0.09 \tag{A.14}$$

while for the second one, the violation is preserved for $(1-p)2\sqrt{2}(N-1) > 2(N-1)$; hence

$$p'_{max}(\mathcal{I}^2_{mix}) = 1 - \frac{\sqrt{2}}{2} \approx 0.29 \tag{A.15}$$

Clearly, we see that for the second setting a higher violation results also in a significantly higher robustness to noise.

Appendix B

Appendix of Chapter 4

B.1 Projecting the vertices of the k-producible polytopes

Here we show in more detail how to explicitly project the vertices of the k-producible polytopes and obtain the expressions in (4.7) and in (4.8). Let us start by recalling that, for any fixed L_k-partition, the corresponding vertices of the $\mathcal{P}_{N,k}$ factorise in the following way

$$p(\mathbf{a}|\mathbf{x}) = p_1(\mathbf{a}_{\mathcal{A}_1}|\mathbf{x}_{\mathcal{A}_1}) \cdot \ldots \cdot p_L(\mathbf{a}_{\mathcal{A}_L}|\mathbf{x}_{\mathcal{A}_L}) \tag{B.1}$$

where each $p_s(\mathbf{a}_{\mathcal{A}_s}|\mathbf{x}_{\mathcal{A}_s})$ being a vertex of the corresponding $|\mathcal{A}_s|$-partite nonsignaling polytope. As explained in Section 2.1.2, the vertices of the projected polytope $\mathcal{P}^{2,S}_{N,k}$ can be obtained directly by projecting the original vertices into the two-body symmetric space. In other words, we simply have to compute the symmetric correlators (4.2) as function of (B.1). Let us start by evaluating the one-body correlators as follows

$$S_x = \sum_{i=1}^{N} \langle M_x^{(i)} \rangle = \sum_{\mathcal{A}_s} \sum_{i \in \mathcal{A}_s} \langle M_x^{(i)} \rangle = \sum_{p=1}^{k} \sum_{\substack{\mathcal{A}_s \\ s.t. |\mathcal{A}_s| = p}} \sum_{i \in \mathcal{A}_s} \langle M_x^{(i)} \rangle \tag{B.2}$$

where we have first divided the summation into parties belonging to the same partition $\mathcal{A}_s$ and then further grouped the partitions of same size. Notice now that

$$\sum_{i \in \mathcal{A}_s} \langle M_x^{(i)} \rangle = S_x(p_s(\mathbf{a}_{\mathcal{A}_s}|\mathbf{x}_{\mathcal{A}_s})) \tag{B.3}$$

where we denote by $S_x(p_s(\mathbf{a}_{\mathcal{A}_s}|\mathbf{x}_{\mathcal{A}_s}))$ the one-body components of the vector in the symmetric two-body space, obtained by projecting the vertex $p_s(\mathbf{a}_{\mathcal{A}_s}|\mathbf{x}_{\mathcal{A}_s}))$ only. Notice that the list of extremal points resulting

from the projection of the vertices of the p-partite no-signaling polytope coincides with the vertices of the projected set $\mathcal{NS}_p^{2,S}$. Hence we can rewrite (B.2) as

$$S_x = \sum_{p=1}^{k} \sum_{\substack{\mathcal{A}_s \\ s.t.|\mathcal{A}_s|=p}} S_x(p, i_{\mathcal{A}_s}) \tag{B.4}$$

where we have now adopted the notation in (4.5) for the vector denoting a given vertex of the projected no-signaling polytope and $i_{\mathcal{A}_s} = 1, \ldots, n_p$ can run over all the possible choices of vertices. Now, to list all the extremal points of $\mathcal{P}_{N,k}^{2,S}$, we have to consider all the possible L_k-partitions of N parties. Notice, however, that the expression in (B.4) is now invariant under permutation of parties, since it is a function of the symmetric S_x terms only. This property allows for further simplifications: indeed, it implies that the vertices components $\mathcal{S}_x$ are sensitive only to how many partitions of same size p are associated to the same projected vertex $S_x(p, i)$, while being insensitive to which specific parties belong to such partitions. Therefore, we introduce the concept of populations $\xi_{p,i}$, which are integer numbers counting how many, among the partitions of size p, are associated to the same vertex $S_x(p, i)$. Clearly, if multiplied by p, the population have to sum to the actual number of parties belonging to these partitions. Moreover, if we sum over the different sizes, we obtain the total number of particles. These conditions can be summarised by the following equation

$$\sum_{p=1}^{k} \sum_{i=1}^{n_p} p\, \xi_{p,i} = N. \tag{B.5}$$

and (B.4) can now be restated as

$$S_x = \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i} S_x(p, i) \tag{B.6}$$

In this formalism, running over all the choices of population satisfying (B.5) corresponds to listing all the non-equivalent choices of L_k-partitions.

Now that the one-body terms have been computed, we use a similar argument to compute the two-body components as function of the population and the projected components $S_{xy}(p, i)$. Following from (4.2), we have

$$S_{xy} = \sum_{\substack{i,j=1 \\ i \neq j}}^{N} \langle M_x^{(i)} M_y^{(j)} \rangle = \sum_{\mathcal{A}_s} \sum_{\substack{i,j \in \mathcal{A}_s \\ i \neq j}} \langle M_x^{(i)} M_y^{(j)} \rangle + \sum_{\substack{\mathcal{A}_s, \mathcal{A}_t \\ s \neq t}} \langle M_x^{(i)} \rangle \langle M_y^{(j)} \rangle \tag{B.7}$$

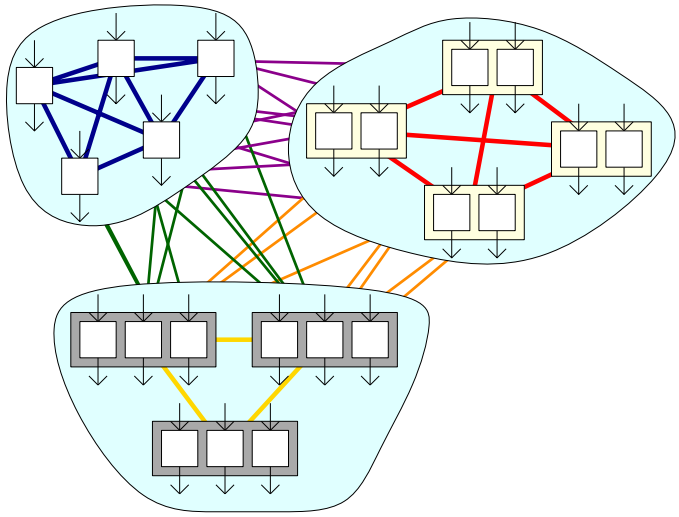

Figure B.1: An example with $N = 22$, and the 3-partition into $n_1 = 5$ sets of size 1, $n_2 = 4$ of size 2 and $n_3 = 3$ of size 3. The first sum in Eq. (B.9) corresponds to the value of S_{xy} that comes from the two-body correlators $\langle M_x^{(i)} M_y^{(j)} \rangle$ within each set (i.e., $i, j \in \mathcal{A}_l$ for some l). For the 1-body boxes, these values are clearly zero, and for larger boxes, they correspond to the two-body marginals of the corresponding Popescu-Rohrlich box (PR-box). Therefore, once symmetrised, the contribution of the box involving p parties using the i-th strategy is $S_{xy}(p, i)$. The second sum in Eq. (B.9) counts those two-body correlators $\langle M_x^{(i)} M_y^{(j)} \rangle$ in which $i \in \mathcal{A}_k$, $j \in \mathcal{A}_l$, $k \neq l$ and $|\mathcal{A}_k| = |\mathcal{A}_l| = p$. These correlations are represented by the blue, red and yellow lines. Because they are correlations coming from different PR-boxes, the locality assumption guarantees the factorisation $\langle M_x^{(i)} M_y^{(j)} \rangle = \langle M_x^{(i)} \rangle \langle M_y^{(j)} \rangle$, yielding the term $S_x(p, i) S_y(p, i)$ once symmetrised. The factor $\xi_{p,i}(\xi_{p,i} - 1)$ is given by the fact that $\mathcal{S}_{xy}$ is defined as the sum for all $i \neq j$, therefore containing repetitions. Finally, the last sum in Eq. (B.9) is given by all two-body correlators $\langle M_x^{(i)} M_y^{(j)} \rangle$ in which $i \in \mathcal{A}_k$, $j \in \mathcal{A}_l$, and $|\mathcal{A}_k| = p$, $|\mathcal{A}_l| = q$ with $p \neq q$, i.e., two-body correlations connecting PR-boxes of different size. Here the locality assumption also enables a factorisation which amounts to $S_x(p, i) S_y(q, j)$ once symmetrised, weighted by the number of occurrences $\xi_{p,i} \xi_{q,j}$. These correspond to the purple, green and orange lines in the figure.

where we have used that, because of the factorisation (B.1), the two-body expectation values factorise as well when i, j belong to different partitions. Similarly to the one-body case, we then group partitions of same sizes and substitute the sum over parties with the symmetrised correlator, so

to get

$$\begin{aligned} S_{xy} &= \sum_{p=1}^{k} \sum_{\substack{\mathcal{A}_s \\ s.t.|\mathcal{A}_s|=p}} S_{xy}(p, i_{\mathcal{A}_s}) \\ &+ \sum_{p=1}^{k} \sum_{\substack{\mathcal{A}_s,\mathcal{A}_t \\ s.t.|\mathcal{A}_s|=|\mathcal{A}_t|=p \\ s\neq t}} S_x(p, i_{\mathcal{A}_s}) S_y(p, i_{\mathcal{A}_t}) \\ &+ \sum_{\substack{p,q=1 \\ p\neq q}}^{k} \sum_{\substack{\mathcal{A}_s,\mathcal{A}_t \\ s.t.|\mathcal{A}_s|=p \\ |\mathcal{A}_t|=q}} S_x(p, i_{\mathcal{A}_s}) S_y(q, i_{\mathcal{A}_t}) \end{aligned} \tag{B.8}$$

Notice that we have divided the second sum in (B.7) into the case where the two partitions $\mathcal{A}_s, \mathcal{A}_t$ are of same or different size. Lastly, we replace the sum over different vertices (B.1) and all the L_k-partitions with the sum over population and we arrive at

$$\begin{aligned} S_{xy}(\vec{\xi}) &= \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i} S_{xy}(p,i) + \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i}(\xi_{p,i}-1) S_x(p,i) S_y(p,i) \\ &+ \sum_{\{p,i\}\neq\{q,j\}} \xi_{p,i}\xi_{q,j} S_x(p,i) S_y(q,j), \end{aligned} \tag{B.9}$$

B.2 Vertices of the projected nonsignaling polytopes of $N = 2, 3, 4$ particles

Here we attach tables with vertices for the projections $\mathcal{NS}_N^{2,S}$ of the nonsignaling polytopes $\mathcal{NS}_N$ onto the symmetric two-body subspace for $2 \leq N \leq 4$ (Tables B.2–B.4). For completeness we also attach the table containing the deterministic values of single-body correlations (Table B.1). We omit the cases $N = 5, 6$ because the lists of vertices are too long to present it here.

Notice that, for the smallest Ns, the lists of vertices of the no-signaling polytopes are known. For $N = 2$, the only nonlocal vertices belong to the equivalence class of the so-called PR-box [PR94]. For $N = 3$, the list of the 46 equivalence classes was derived in [PBS11]. Therefore, for these scenarios, the projection can be performed straightforwardly through the vertex representation (cfr. Section 2.1.2). The resulting extremal points are shown in Table B.2 and B.3 in (the vertices that are shared with the local polytope are omitted). For the bipartite case,

$N = 2$, the 4 non-trivial vertices belong obviously to a single equivalence class, corresponding to the projection of the PR-box. Interestingly, there is also only one relevant class for the tripartite case, corresponding to the projection of the class number 29 of [PR94], which is one of the two that violate maximally the Guess-Your-Neighbour-Input inequality [ABB$^+$10]. For higher values of N the number of equivalence classes starts growing, as it can already be seen for the vertices of $N = 4$ in Table B.4.

	S_0	S_1	S_{00}	S_{01}	S_{11}
$\xi_{1,1}$	1	1	0	0	0
$\xi_{1,2}$	1	-1	0	0	0
$\xi_{1,3}$	-1	1	0	0	0
$\xi_{1,4}$	-1	-1	0	0	0

Table B.1: List of the values of the one- and two-body symmetric expectation values for deterministic local strategies. In this case S_0 and S_1 contain consist of one expectation value, while S_{xy} are simply zero.

	S_0	S_0	S_{00}	S_{01}	S_{11}
$\xi_{2,1}$	0	0	2	2	-2
$\xi_{2,1}$	0	0	-2	2	2
$\xi_{2,3}$	0	0	2	-2	-2
$\xi_{2,4}$	0	0	-2	-2	2

Table B.2: List of the vertices of $\mathcal{NS}_2^{2,S}$. In the first column we also add the corresponding populations.

B.3 Deriving the inequality for k-nonlocality for any number of parties

In what follows we explicitly compute k-producible bounds β_k [cfr. Eq. (4.4)] for different k's for the two-body Bell expression (4.19). We begin with fully general considerations and later we focus on a few values of k and compute β_k case by case. Let us start by noting that, since the sets $\mathcal{P}_{N,k}^{2,S}$ are polytopes, it is enough to perform the above minimisation over their vertices. Hence, by making use of Eqs. (4.7) and (B.9), the

	S_0	S_0	S_{00}	S_{01}	S_{11}
$\xi_{3,1}$	-1	-1	6	-2	-2
$\xi_{3,2}$	-1	-1	-2	-2	6
$\xi_{3,3}$	-1	1	6	2	-2
$\xi_{3,4}$	-1	1	-2	2	6
$\xi_{3,5}$	1	-1	6	2	-2
$\xi_{3,6}$	1	-1	-2	2	6
$\xi_{3,7}$	1	1	6	-2	-2
$\xi_{3,8}$	1	1	-2	-2	6

Table B.3: List of the vertices of $\mathcal{NS}_3^{2,S}$. In the first column we also add the corresponding populations.

	S_0	S_0	S_{00}	S_{01}	S_{11}
$\xi_{4,1}$	-2	-2	12	0	0
$\xi_{4,2}$	-2	-2	0	0	12
$\xi_{4,3}$	-2	2	12	0	0
$\xi_{4,4}$	-2	2	0	0	12
$\xi_{4,5}$	2	-2	12	0	0
$\xi_{4,6}$	2	-2	0	0	12
$\xi_{4,7}$	2	2	12	0	0
$\xi_{4,8}$	2	2	0	0	12
$\xi_{4,9}$	0	0	12	-4	-4
$\xi_{4,10}$	0	0	-4	-4	12
$\xi_{4,11}$	0	0	12	4	-4
$\xi_{4,12}$	0	0	-4	4	12
$\xi_{4,13}$	$\frac{-20}{7}$	$\frac{-4}{7}$	$\frac{36}{7}$	$\frac{-12}{7}$	$\frac{-12}{7}$
$\xi_{4,14}$	$\frac{-20}{7}$	$\frac{-4}{7}$	$\frac{-12}{7}$	$\frac{-12}{7}$	$\frac{36}{7}$
$\xi_{4,15}$	$\frac{-20}{7}$	$\frac{4}{7}$	$\frac{36}{7}$	$\frac{12}{7}$	$\frac{-12}{7}$
$\xi_{4,16}$	$\frac{-20}{7}$	$\frac{4}{7}$	$\frac{-12}{7}$	$\frac{12}{7}$	$\frac{36}{7}$
$\xi_{4,17}$	$\frac{20}{7}$	$\frac{-4}{7}$	$\frac{36}{7}$	$\frac{12}{7}$	$\frac{-12}{7}$
$\xi_{4,18}$	$\frac{20}{7}$	$\frac{-4}{7}$	$\frac{-12}{7}$	$\frac{12}{7}$	$\frac{36}{7}$
$\xi_{4,19}$	$\frac{20}{7}$	$\frac{4}{7}$	$\frac{36}{7}$	$\frac{-12}{7}$	$\frac{-12}{7}$
$\xi_{4,20}$	$\frac{20}{7}$	$\frac{4}{7}$	$\frac{-12}{7}$	$\frac{-12}{7}$	$\frac{36}{7}$

Table B.4: List of the vertices of $\mathcal{NS}_4^{2,S}$. In the first column we also present the associated populations.

expression $\mathcal{I}$ in Eq. (4.19) for all vertices of $\mathcal{P}^{2,S}_{N,k}$ can be written as

$$\mathcal{I}(\vec{S}(\vec{\xi})) = \sum_{p=1}^{k}\sum_{i=1}^{n_p}\xi_{p,i}\mathcal{I}(\vec{S}(p,i)) + \frac{1}{2}\sum_{p=1}^{k}\sum_{i=1}^{n_p}\xi_{p,i}\left[\xi_{p,i}-1\right]\mathcal{I}(\vec{S}(p,i),\vec{S}(p,i)) + \\ + \frac{1}{2}\sum_{\{p,i\}\neq\{q,j\}}\xi_{p,i}\xi_{q,j}\mathcal{I}(\vec{S}(p,i),\vec{S}(q,j)), \tag{B.10}$$

where we have defined the following cross-terms

$$\mathcal{I}(\vec{S}(p,i),\vec{S}(q,j)) = \left[S_0(p,i)+S_1(p,i)\right]\left[S_0(q,j)+S_1(q,j)\right]. \tag{B.11}$$

When the vectors $\vec{S}(p,i)$ are known, the expression (B.10) takes the form of a polynomial of degree two in terms of the populations $\xi_{p,i}$. By grouping together the linear and quadratic terms, we get

$$\mathcal{I}(\vec{S}(\vec{\xi})) = \sum_{p=1}^{k}\sum_{i=1}^{n_p}\xi_{p,i}\left[\mathcal{I}(\vec{S}(p,i)) - \frac{1}{2}\mathcal{I}(\vec{S}(p,i),\vec{S}(p,i))\right] + \\ \frac{1}{2}\sum_{p,q=1}^{k}\sum_{i,j=1}^{n_p}\xi_{p,i}\xi_{q,j}\mathcal{I}(\vec{S}(p,i),\vec{S}(q,j)) \tag{B.12}$$

Then, by substituting the explicit form of the cross-term (B.11), one arrives at

$$\mathcal{I}(\vec{S}(\vec{\xi})) = \sum_{p=1}^{k}\sum_{i=1}^{n_p}\xi_{p,i}\left\{\mathcal{I}(\vec{S}(p,i)) - \frac{1}{2}[S_0(p,i)+S_1(p,i)]^2\right\} + \\ \frac{1}{2}\left\{\sum_{p=1}^{k}\sum_{i=1}^{n_p}\xi_{p,i}[S_0(p,i)+S_1(p,i)]\right\}^2. \tag{B.13}$$

With the above expression at hand we can now seek the k-producibility bounds β_k for $\mathcal{I}$. Our approach is the following. Instead of minimising the expression $\mathcal{I}$ for all k-producible correlations, we will rather consider a particular value of β_k and prove that the inequality $\mathcal{I}+\beta_k \geq 0$ holds for all integer values of $\xi_{p,i} \geq 0$ for $p = 1,\ldots,k$ and $i = 1,\ldots,n_p$ such that the condition (4.6) holds.

B.3.1 Cases $k = 2$ and $k = 3$

We will first consider the simplest cases of $k = 2, 3$ and show that for them $\beta^k_C = 2N$ is the correct classical bound. In other words, below we demonstrate the following inequality

$$2S_0 + \frac{1}{2}S_{00} + S_{01} + \frac{1}{2}S_{11} + 2N \geq 0 \tag{B.14}$$

is satisfied for all correlations belonging to $\mathcal{P}^{2,S}_{N,k}$ for $k = 2, 3$ and any N. To this end, we use Eqs. (B.13) and (4.6) to write down the following expression

$$\mathcal{I}(\vec{S}(\vec{\xi})) + 2N = \sum_{p=1}^{k}\sum_{i=1}^{n_p} \xi_{p,i}\left\{\mathcal{I}(\vec{S}(p,i)) + 2p - \frac{1}{2}[S_0(p,i) + S_1(p,i)]^2\right\} + \frac{1}{2}\left\{\sum_{p=1}^{k}\sum_{i=1}^{n_p} \xi_{p,i}[S_0(p,i) + S_1(p,i)]\right\}^2 . \tag{B.15}$$

Then, plugging in the explicit values of the one- and two-body symmetric expectation values for $p = 1, 2, 3$ collected in Tables B.1–B.3, the above further rewrites as

$$\begin{aligned}\mathcal{I}(\vec{S}(\vec{\xi})) + 2N = {} & 2\left[\left(\xi_{1,1} - \xi_{1,4} - \xi_{3,1} - \xi_{3,2} + \xi_{3,7} + \xi_{3,8}\right)^2 + \xi_{1,1} + 2\xi_{1,2} - \xi_{1,4}\right] \\ & +2\left[3\left(\xi_{2,1} + \xi_{2,2}\right) + \xi_{2,3} + \xi_{2,4}\right] \\ & +2\left[\left(\xi_{3,1} + \xi_{3,2}\right) + 4\left(\xi_{3,3} + \xi_{3,4}\right)\right. \\ & \left.+6\left(\xi_{3,5} + \xi_{3,6}\right) + 3\left(\xi_{3,7} + \xi_{3,8}\right)\right].\end{aligned} \tag{B.16}$$

With the following substitutions

$$\begin{aligned}\mathcal{X} &= 2\left(\xi_{1,1} - \xi_{1,4}\right), \\ \mathcal{Y} &= 2\left(-\xi_{3,1} - \xi_{3,2} + \xi_{3,7} + \xi_{3,8}\right), \\ \mathcal{P}(\vec{\xi}) &= 2\left[\xi_{1,2} + 3\left(\xi_{2,1} + \xi_{2,2}\right) + \xi_{2,3} + \xi_{2,4} + 2\left(\xi_{3,1} + \xi_{3,2}\right)\right. \\ &\quad \left.+4\left(\xi_{3,3} + \xi_{3,4}\right) + 6\left(\xi_{3,5} + \xi_{3,6}\right) + 2\left(\xi_{3,7} + \xi_{3,8}\right)\right],\end{aligned} \tag{B.17}$$

we can bring the expression (B.16) into the following simple form

$$\begin{aligned}\mathcal{I}(\vec{S}(\vec{\xi})) + 2N &= \frac{1}{2}\left(\mathcal{X} + \mathcal{Y}\right)^2 + \mathcal{X} + \mathcal{Y} + \mathcal{P}(\vec{\xi}) \\ &= 2\mathcal{Z}(\mathcal{Z}+1) + \mathcal{P}(\vec{\xi}),\end{aligned} \tag{B.18}$$

where $\mathcal{Z} = (\mathcal{X}+\mathcal{Y}/2)$. We then notice that all $\xi_{p,i} \geq 0$, which immediately implies that $\mathcal{P}(\vec{\xi}) \geq 0$ for all configurations of populations. Thus, we are left with the term $\mathcal{Z}(\mathcal{Z}+1)$, which is negative only when $-1 < \mathcal{Z} < 0$. However, due to the fact that $\mathcal{Z}$ is a linear combination of integers with integer coefficients, it cannot take such values. Thus, $\mathcal{Z}(\mathcal{Z}+1) \geq 0$, which completes the proof.

B.3.2 The case $k = 4$

We now address the first case in which the bound β_k is different than the local bound of the Bell inequality. First of all, we notice that the

bipartite nonsignaling populations $\xi_{2,i}$ enter the expression (B.15) only in the linear part and, since their coefficient are always positive, we know that they never contribute to the violation of the local bound. Thus, the expression $\mathcal{I}(\vec{S}(\vec{x}))+2N$ without these terms reads explicitly

$$\begin{aligned}
&\frac{1}{2}\left(\mathcal{X}+\mathcal{Y}+\mathcal{Y}'+\mathcal{W}+\mathcal{W}'\right)^2+2\left(\xi_{1,1}+2\xi_{1,2}-\xi_{1,4}\right)\\
&\quad+2\left[\left(\xi_{3,1}+\xi_{3,2}\right)+4\left(\xi_{3,3}+\xi_{3,4}\right)+6\left(\xi_{3,5}+\xi_{3,6}\right)+3\left(\xi_{3,7}+\xi_{3,8}\right)\right]\\
&\quad+2\left[\xi_{4,1}+\xi_{4,2}+5\left(\xi_{4,3}+\xi_{4,4}\right)+9\left(\xi_{4,5}+\xi_{4,6}\right)+5\left(\xi_{4,7}+\xi_{4,8}\right)\right]\\
&\quad+8\left[\xi_{4,9}+\xi_{4,10}+2\left(\xi_{4,11}+\xi_{4,12}\right)\right]\\
&\quad+\frac{8}{49}\left[-22\left(\xi_{4,13}+\xi_{4,14}\right)+19\left(\xi_{4,15}+\xi_{4,16}\right)\right.\\
&\quad\left.+89\left(\xi_{4,17}+\xi_{4,18}\right)+48\left(\xi_{4,19}+\xi_{4,20}\right)\right],
\end{aligned}\tag{B.19}$$

where $\mathcal{X}$ and $\mathcal{Y}$ are defined above and $\mathcal{Y}'$, $\mathcal{W}$ and $\mathcal{W}'$ are given by

$$\begin{aligned}
\mathcal{Y}' &= 4\left(-\xi_{4,1}-\xi_{4,2}+\xi_{4,7}+\xi_{4,8}\right),\\
\mathcal{W} &= \frac{24}{7}\left(-\xi_{4,13}-\xi_{4,14}+\xi_{4,19}+\xi_{4,20}\right),\\
\mathcal{W}' &= \frac{16}{7}\left(-\xi_{4,15}-\xi_{4,16}+\xi_{4,17}+\xi_{4,18}\right).
\end{aligned}\tag{B.20}$$

Then, we can simplify this expression

$$\frac{1}{2}\left(\mathcal{X}+\mathcal{Y}+\mathcal{Y}'+\mathcal{W}+\mathcal{W}'\right)^2+\mathcal{X}+\mathcal{Y}+\mathcal{Y}'+\mathcal{W}+\mathcal{W}'+\widetilde{\mathcal{P}}(\vec{\xi})-\frac{8}{49}\left(\xi_{4,13}+\xi_{4,14}\right),\tag{B.21}$$

where

$$\begin{aligned}
\widetilde{\mathcal{P}}(\vec{\xi}) &= 4\xi_{2,2}+4\left[\xi_{3,1}+\xi_{3,2}+2\left(\xi_{3,3}+\xi_{3,4}\right)+3\left(\xi_{3,5}+\xi_{3,6}\right)+\xi_{3,7}+\xi_{3,8}\right]\\
&\quad+2\left[3\left(\xi_{4,1}+\xi_{4,2}\right)+5\left(\xi_{4,3}+\xi_{4,4}\right)+9\left(\xi_{4,5}+\xi_{4,6}\right)+3\left(\xi_{4,7}+\xi_{4,8}\right)\right]\\
&\quad+8\left[\xi_{4,9}+\xi_{4,10}+2\left(\xi_{4,11}+\xi_{4,12}\right)\right]\\
&\quad+\frac{8}{49}\left[33\left(\xi_{4,15}+\xi_{4,16}\right)+75\left(\xi_{4,17}+\xi_{4,18}\right)+27\left(\xi_{4,19}+\xi_{4,20}\right)\right]
\end{aligned}\tag{B.22}$$

is a polynomial that is positive for all configurations of populations $\xi_{p,i}$. Let us now show that the expression in (B.22) is always greater or equal to $-2N/49-1/2$. In other words, we want to prove that

$$\begin{aligned}
&\frac{1}{2}\left(\mathcal{X}+\mathcal{Y}+\mathcal{Y}'+\mathcal{W}+\mathcal{W}'\right)^2+\mathcal{X}+\mathcal{Y}+\mathcal{Y}'+\mathcal{W}+\mathcal{W}'+\widetilde{\mathcal{P}}(\vec{\xi})\\
&\qquad-\frac{8}{49}\left(\xi_{4,13}+\xi_{4,14}\right)+\frac{1}{2}+\frac{2}{49}N\geq 0,
\end{aligned}\tag{B.23}$$

for any $\xi_{p,i}$. To this end, we can exploit (4.6) in order to express N in terms of the populations, which allows us to see that $2N\geq 8(\xi_{4,13}+\xi_{4,14})$,

implying that (B.23) holds true. As a result, the bound for $k = 4$ amounts to

$$\beta_C^4 = \left(2 + \frac{2}{49}\right) N + \frac{1}{2}. \tag{B.24}$$

B.3.3 Cases $k = 5, 6$

Based on the previous results our guess is that for any $3 < k < N$, the bound for k-producible correlations is given by

$$\beta_C^k = 2N + \frac{1}{2} + \alpha_k N. \tag{B.25}$$

In what follows we estimate the correction to the linear dependence on N, that is, α_k for $k = 5, 6$, and leave the general case of any k as an open problem. To this aim, we follow the approach used in the case $k = 4$. More precisely, by substituting β_C^k given in (B.25) into $\mathcal{I} + \beta_C^k$, we obtain

$$\begin{aligned}
\mathcal{I}(\vec{S}(\vec{\xi})) + \beta_C^k \;=\; & \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i} \left[\mathcal{I}(\vec{S}(p,i)) + (2 + \alpha_k)\, p - \frac{1}{2} \left[S_0(p,i) + S_1(p,i) \right]^2 \right] \\
& + \frac{1}{2} \left\{ \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i} \left[S_0(p,i) + S_1(p,i) \right] \right\}^2 + \frac{1}{2} \\
= \; & \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i} \Big\{ \mathcal{I}_6(\vec{S}(p,i)) + (2 + \alpha_k)\, p \\
& \qquad - \frac{1}{2} \left[S_0(p,i) + S_1(p,i) \right]^2 - \left[S_0(p,i) + S_1(p,i) \right] \Big\} \\
& + \frac{1}{2} \left\{ \sum_{p=1}^{k} \sum_{i=1}^{n_p} \xi_{p,i} \left[S_0(p,i) + S_1(p,i) \right] + 1 \right\}^2 .
\end{aligned} \tag{B.26}$$

As the last term in this expression is always nonnegative, to study the positivity of $\mathcal{I}(\vec{S}(\vec{\xi})) + \beta_C^{(k)}$, we can restrict our attention to the following function

$$\begin{aligned}
\Omega(\vec{\xi}) = \sum_{p=1}^{k} \sum_{i=1}^{n_p} \quad & \xi_{p,i} \Big\{ \mathcal{I}(\vec{S}(p,i)) + (2 + \alpha_k)\, p \\
& - \frac{1}{2} \left[S_0(p,i) + S_1(p,i) \right]^2 - \left[S_0(p,i) + S_1(p,i) \right] \Big\} .
\end{aligned} \tag{B.27}$$

As it is a linear function in the populations which are all nonnegative, its minimum is reached for the population ξ^* standing in front the expression that takes the minimal value over all choices of the vertices. In other words, we can lower bound $\Omega(\vec{x})$ as

$$\Omega(\vec{\xi}) \geq \xi^*(p^*\alpha_k + m_k), \tag{B.28}$$

where p^* is the number of parties corresponding to x^* and m_k is defined as

$$m_k = \min_{p=1,\ldots,k} \min_{i=1,\ldots,n_p} \Big\{ \mathcal{I}(\vec{S}(p,i)) + 2p - \frac{1}{2}[S_0(p,i) + S_1(p,i)]^2 - [S_0(p,i) + S_1(p,i)] \Big\}. \tag{B.29}$$

Thus, we simply need to compute m_k and the value α_k we are looking for can be taken as $\alpha_k = m_k/k$ as for it $\Omega(\vec{\xi}) \geq 0$ for any N.

To this end, we perform the minimisation in (B.29) by evaluating the right-hand side on each vertex of the projected five- and six-partite no-signaling polytope. We obtain $m_5 = 40/121$ and $m_6 = 1/2$, implying that the modified bounds amount to

$$\beta_C^5 = \left(2 + \frac{8}{121}\right) N + \frac{1}{2}, \tag{B.30}$$

and

$$\beta_C^6 = \left(2 + \frac{1}{12}\right) N + \frac{1}{2}, \tag{B.31}$$

respectively.

B.4 Estimating the Svetlichny and Mermin operators with collective spin measurements

Here we show the details on the derivation of the witnessed for the Mermin and Svetlichny inequalities in (4.24) and (4.22). Their fully local β_1, the k-nonlocal $beta_k$, the quantum β_Q and the nonsignaling bounds are given in Table B.5 and B.6.

local β_C	k-nonlocal β_k	quantum β_Q	nonsignaling β_{NS}
$2^{\frac{1-(-1)^N}{4}}$	$2^{(N-2\lfloor\frac{\lceil N/k\rceil}{2}\rfloor)/2}$	$2^{(N-1)/2}$	$2^{N/2}$

Table B.5: The local β_C, k-nonlocal β_k, quantum β_Q and nonsignaling bounds for the Svetlichny Bell expression.

local β_C	k-nonlocal β_k	quantum β_Q	nonsignaling β_{NS}
$2^{\frac{1+(-1)^N}{4}}$	$2^{(N-2\lfloor\frac{\lceil N/k\rceil+1}{2}\rfloor+1)/2}$	$2^{(N-1)/2}$	$2^{(N-1)/2}$

Table B.6: The local β_C, k-nonlocal β_k, quantum β_Q and nonsignaling bounds for the Mermin Bell expression.

Generally, the bounds for these inequalities are expressed in terms of the number of groups m in which the N parties are splitted. Noticing that N, m and k are related by the relation $m + k - 1 \leq N \leq mk$ allows one to express the bound as a function of the nonlocality depth k (resulting in the bound in the table above). The fact that these bounds can be achieved with a model in which $\lfloor N/k \rfloor$ groups contain exactly k parties implies that the resulting bounds are tight [BBGP09]. As the quantum bound is larger than the $(N-1)$-nonlocal bound, the Mermin and Svetlichny expressions can reveal genuine multipartite nonlocality. .

The measurement settings maximising the quantum value of the Svetlichny inequality, for a $|\mathrm{GHZ}_N^+\rangle$ state, $\left|\mathrm{GHZ}_N^\pm\right\rangle = (|0\rangle^{\otimes N} \pm |1\rangle^{\otimes N})/\sqrt{2}$, are

$$M_j^{(i)} = \cos(\phi_j)\, X + \sin(\phi_j)\, Y \ , \qquad \phi_j = -\frac{\pi}{4N} + j\frac{\pi}{2} \tag{B.32}$$

with $j \in 0, 1,$. By substituting in the inequality (4.22), we find that the Svetlichny operator takes the following very simple form

$$\mathcal{B}_N^{\mathrm{Svet}} = 2^{(N-1)/2} \left(|0\rangle\langle 1|^{\otimes N} + |1\rangle\langle 0|^{\otimes N}\right). \tag{B.33}$$

If the mean value of this operator $\mathrm{tr}(\rho\mathcal{B}_N^{\mathrm{Svet}})$ is larger than the k-nonlocal bound given in the table above, we conclude that the state ρ has the capability to violate a Svetlichny inequality with the corresponding bound, that is, ρ is $(k+1)$-Bell correlated. Similarly, to maximally violate the Mermin inequality with a GHZ state, we choose $M_0^{(i)} = X$ and $M_1^{(i)} = Y$ for each party $i = 1, \ldots N$, and for them the Bell operator reduces indeed to the same Bell operator as before, that is,

$$\mathcal{B}_N^{\mathrm{Mermin}} = 2^{(N-1)/2} \left(|0\rangle\langle 1|^{\otimes N} + |1\rangle\langle 0|^{\otimes N}\right). \tag{B.34}$$

In order to state our bound in (4.26), we first need to prove that the following operator

$$\begin{aligned}\chi_N =& |\mathrm{GHZ}_N^+\rangle\langle\mathrm{GHZ}_N^+| - |\mathrm{GHZ}_N^-\rangle\langle\mathrm{GHZ}_N^-| - \underbrace{X_1 \ldots X_N}_{N \text{ times}} \\ & - \sum_{m\neq n}^{N} Z_m Z_n + N(N-1)\mathbb{1}\end{aligned} \tag{B.35}$$

is positive semi-definite, where X_i/Z_i stands for the Pauli matrix X/Z acting on site i. The proof can be derived in various ways from [TG05a], this reference focusing on genuine entanglement detection.

To this aim, let us assume for simplicity N to be even and consider the GHZ state $|\mathrm{GHZ}_N^+\rangle$, and the following set of states obtained by flipping k of its spins with $k = 1, \ldots, N/2$, that is

$$\begin{aligned}
&X_{i_1}|\mathrm{GHZ}^+\rangle, \\
&X_{i_1}X_{i_2}|\mathrm{GHZ}^+\rangle, && i_1 \neq i_2 \\
&\qquad\vdots \\
&X_{i_1}X_{i_2}\ldots X_{i_{N/2-1}}|\mathrm{GHZ}^+\rangle, && i_1 \neq i_2 \neq \ldots \neq i_{N/2-1} \\
&X_{i_1}X_{i_2}\ldots X_{i_{N/2}}|\mathrm{GHZ}^+\rangle, && i_1 \neq i_2 \neq \ldots \neq i_{N/2}
\end{aligned} \tag{B.36}$$

where $i_\ell = 1, \ldots, N$ for $\ell = 1, \ldots, N/2$. Notice that in each "line" of Eq. (B.36) there are $C_N^k = \binom{N}{k}$ $(k = 1, \ldots, N/2-1)$ orthogonal states except for the last one in which the number of orthogonal vectors is $C_N^{N/2}/2$. We then construct an analogous set of vectors with $|\mathrm{GHZ}_N^-\rangle$, which altogether gives us a set of

$$2\sum_{k=0}^{N/2-1} C_N^k + C_N^{N/2} = \sum_{k=0}^{N} C_N^k = 2^N$$

orthonormal vectors forming a basis in $(\mathbb{C}^2)^{\otimes N}$. Let us now show that the operator χ_N is diagonal in this basis. For this purpose, we notice that $XZX = -Z$ and therefore (see also Ref. [SG01])

$$\begin{aligned}
&\langle \mathrm{GHZ}_N^\pm|(X_{i_1}X_{i_2}\ldots X_{i_\ell})\,(Z_mZ_n)\,(X_{i_1}X_{i_2}\ldots X_{i_\ell})|\mathrm{GHZ}_N^\pm\rangle \\
&= (-1)^{\lambda_{m,n}}\,\mathrm{tr}\left(Z_mZ_n|\mathrm{GHZ}_N^\pm\rangle\langle\mathrm{GHZ}_N^\pm|\right) = (-1)^{\lambda_{m,n}},
\end{aligned}$$

where $\ell = 1, \ldots, N/2$, $m \neq n$, and $\lambda_{m,n} = 0$ if both qubits m and n are flipped or neither of them, and $\lambda_{m,n} = -1$ if only one of them is flipped. We also notice that for the parity operator one has

$$\langle \mathrm{GHZ}_N^\pm|(X_{i_1}X_{i_2}\ldots X_{i_\ell})\,(X_1\ldots X_N)\,(X_{i_1}X_{i_2}\ldots X_{i_\ell})|\mathrm{GHZ}_N^\pm\rangle = \pm 1.$$

All this means that the operator χ_N is diagonal in the above basis. Furthermore, the maximal eigenvalue of $X_1\ldots X_N + \sum_{m\neq n}^N Z_mZ_n$ is $N(N-1)+1$ and the corresponding eigenstate is $|\mathrm{GHZ}_N^+\rangle$. Then, the other GHZ state $|\mathrm{GHZ}_N^-\rangle$ corresponds to the eigenvalue $N(N-1)-1$ and all the other elements of the above basis vectors eigenvectors with

eigenvalues smaller or equal to $N(N-1)-1$. As a result, all eigenvalues of χ_N are non-negative, and hence

$$\begin{aligned}\mathcal{B}_N^{\text{Svet}} = \mathcal{B}_N^{\text{Mermin}} &= \sqrt{2}^{N-1}\left(|\text{GHZ}_N^+\rangle\langle\text{GHZ}_N^+| - |\text{GHZ}_N^-\rangle\langle\text{GHZ}_N^-|\right) \\ &\geq \sqrt{2}^{N-1}\left[X_1\dots X_N + \textstyle\sum_{m\neq n}^N Z_m Z_n - N(N-1)\mathbb{1}\right] \quad \text{(B.37)}\end{aligned}$$

It is not difficult to see that the same reasoning holds for odd N (in this case, the basis is formed with all possible spin flips of $(N-1)/2$ spins), and consequently the above bound is valid for any N. Noticing then that $\sum_{m\neq n}^N Z_m Z_n = 4S_z^2 + N\mathbb{1}$, where $J_z = (1/2)\sum_{i=1}^N Z_i$ is the total spin component along the z axis, we arrive at the following operator bound for the Svetlichny and Mermin Bell operators

$$\begin{aligned}\mathcal{B}_N^{\text{Svet}} = \mathcal{B}_N^{\text{Mermin}} &= \sqrt{2}^{N-1}\left(|\text{GHZ}_N^+\rangle\langle\text{GHZ}_N^+| - |\text{GHZ}_N^-\rangle\langle\text{GHZ}_N^-|\right) \\ &\geq \sqrt{2}^{N-1}\left[X_1\dots X_N + 4J_z^2 - N^2\mathbb{1}\right]. \quad \text{(B.38)}\end{aligned}$$

Combining the k-nonlocal bounds of the Svetlichny and Mermin Bell expressions then allows us to write the following witness of Bell correlations depth:

$$\langle\mathcal{B}_N\rangle = \sqrt{2}^{N-1}\left\langle X_1\dots X_N + 4J_z^2 - N^2\mathbb{1}\right\rangle \leq 2^{(N-\lceil\frac{N}{k}\rceil)/2}. \quad \text{(B.39)}$$

B.5 Complete list of facets for the GMNL polytopes

Here we present the complete list of facets for the polytopes that test for genuine multipartite nonlocality for $N = 3, 4, 5$. We omit the $N = 6, 7$ cases since the amount of inequalities starts becoming too long to be contained in one page. The inequalities are sorted in equivalence classes, under symmetry operations such as outcome/input swapping, in the same fashion as in [TAS+14].

β_C	α	β	γ	δ	ϵ
1	0	0	1	0	0
12	-3	1	3	$-\frac{3}{2}$	-2
6	-2	-2	0	1	0
3	0	0	0	-1	1
3	0	-2	0	0	1
3	0	0	-1	0	0

Table B.7: List of the facets of the symmetric two-body polytope of 2-producible correlations for $N = 3$

β_C	α	β	γ	δ	ϵ
2	1	0	1	0	0
42	12	3	6	2	-3
42	-12	9	6	-6	1
20	-5	3	4	-3	0
30	-6	3	6	-4	-1
12	0	0	3	1	-1
12	3	3	1	2	1
6	-3	0	1	0	0
8	-3	-1	2	1	0
6	0	0	1	-1	0
8	0	2	1	1	1
12	-3	-3	0	1	0
6	0	0	-1	0	0

Table B.8: List of the facets of the symmetric two-body polytope of 3-producible correlations for $N = 4$

β_C	α	β	γ	δ	ϵ
30	-4	10	1	-2	3
40	-8	12	1	-3	3
116	28	-28	4	-9	4
134	-36	30	8	-11	4
452	-120	104	25	-37	15
562	-144	136	27	-45	22
112	28	-28	5	-9	5
116	28	-28	5	-10	5
380	-92	84	21	-34	13
36	-4	8	4	-3	2
380	-92	84	20	-33	12
320	-76	68	20	-29	10
200	-52	44	12	-17	6
16	-2	4	2	-1	1
110	-30	24	7	-9	3
20	4	-4	0	-1	0
410	-120	72	40	-30	3
170	-60	24	20	-10	1
8	0	0	2	1	0
20	0	0	3	3	1
20	-2	8	0	-1	3
20	0	4	1	-2	3
50	0	12	4	-4	5
40	-4	12	2	-3	4
80	4	12	9	-8	7
34	2	6	4	-3	3
4	2	0	1	0	0
10	-4	0	1	0	0
220	60	12	20	5	-8
120	20	-4	20	-5	-6
400	-60	36	60	-45	2
20	4	2	3	2	0
20	-4	-4	1	2	1
80	8	20	-2	5	10
40	-12	-6	5	3	0
2	0	0	0	0	1
10	0	0	-1	0	0

Table B.9: List of the facets of the symmetric two-body polytope of 4-producible correlations for $N = 5$

Appendix C

Appendix of Chapter 5

C.1 Increasing the quantum violation

Here we explain in more detail how our Bell inequalities can be modified to allow for higher ratios β_G^Q/β_G^C.

Given a Bell inequality (5.4) corresponding to a graph G, consider a vertex $j \in V$ that neither belongs to $n(1)$ nor it shares a neighbour with the first vertex. Then one can apply a second substitution $X_j \to M_0^{(j)} + M_1^{(j)}$ and $Z_j \to M_0^{(j)} - M_1^{(j)}$ at that vertex. This gives us the following Bell inequality

$$\begin{aligned} I_G : \;=\; & n_{\max} \left\langle (M_0^{(1)} + M_1^{(1)}) \prod_{i\in n(1)} M_1^{(i)} \right\rangle \\ & + \sum_{i\in n(1)} \left\langle (M_0^{(1)} - M_1^{(1)}) M_0^{(i)} \prod_{j\in n(i)\setminus\{1\}} M_1^{(j)} \right\rangle \\ & + n_j \left\langle (M_0^{(j)} + M_1^{(j)}) \prod_{i\in n(j)} M_1^{(j)} \right\rangle \\ & + \sum_{i\in n(j)} \left\langle (M_0^{(j)} - M_1^{(j)}) M_0^{(i)} \prod_{k\in n(i)\setminus\{j\}} M_1^{(k)} \right\rangle \\ & + \sum_{i\notin n(1)\cup\{1\}\cup n(j)\cup\{j\}} \left\langle M_0^{(i)} \prod_{k\in n(i)} M_1^{(j)} \right\rangle \leq \beta_G^C, \end{aligned} \tag{C.1}$$

for which, as before, it is not difficult to analytically compute the maximal quantum and classical values. They read

$$\beta_{G,Q}^{(2)} = N + n_{max} + n(j) - 2 \tag{C.2}$$

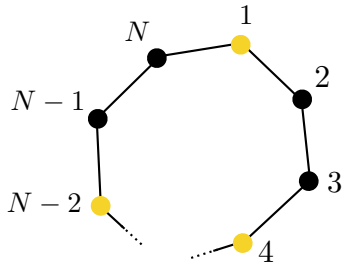

Figure C.1: Pictorial representation of the method to generate Bell inequalities with higher quantum violation, taking the ring graph state. The vertices coloured in yellow are the ones for which the substitution $X_j \to M_0^{(j)} + M_1^{(j)}$ and $Z_j \to M_0^{(j)} - M_1^{(j)}$ is applied.

and

$$\beta_{G,C}^{(2)} = (2\sqrt{2}-1)[n_{max} + n(j)] + N - 2, \tag{C.3}$$

respectively, where the superscript indicates the fact we have played our trick with two sites. It then follows that $\beta_{G,Q}^{(2)}/\beta_{G,C}^{(2)} \geq \beta_G^Q/\beta_G^C$ for any graph G.

We can repeat the same procedure with any other vertex which does not belong to $n(1)$ nor $n(j)$ and does not share any neighbour with neither vertex 1 nor j. In such a way we can increase the ratio again. This clearly comes at the cost of increasing the number of expectation values appearing in the Bell expression. Notice, however, that their linear scaling with N is preserved even in the case in which the above mentioned substitution is applied to any available vertex. Indeed, consider the extremal case in which the replacement with $M_0^{(i)} \pm M_1^{(i)}$ appears for some party i in all the terms in the sum in (5.4). Since such terms correspond to the N generators G_i of the stabilizer group, the resulting amount of correlators is exactly $2N$. One can use a similar argument to see that the ratio β_G^Q/β_G^C is always bounded and cannot exceed $\sqrt{2}$.

As an illustrative example let us turn back to the inequality (5.16) for the ring graph state. To improve the quantum-classical ratio, our methods tells us to choose a vertex whose neighbourhood does not intersect with $n(1) \cup \{1\}$. As a candidate to apply the second substitution we take

vertex 4 so to obtain the following Bell inequality

$$\begin{aligned} I^{(2)}_{\text{ring}} \;:=\; & 2\langle M_1^{(N)}(M_0^{(1)}+M_1^{(1)})M_1^{(2)}\rangle + \langle (M_0^{(1)}-M_1^{(1)})M_0^{(2)}M_1^{(3)}\rangle \\ & + \langle M_1^{(N-1)}M_0^{(N)}(M_0^{(1)}-M_1^{(1)})\rangle + 2\langle M_1^{(3)}(M_0^{(4)}+M_1^{(4)})M_1^{(5)}\rangle + \\ & \langle (M_0^{(4)}-M_1^{(4)})M_0^{(5)}M_1^{(6)}\rangle + \langle M_1^{(2)}M_0^{(3)}(M_0^{(4)}-M_1^{(4)})\rangle \\ & + \sum_{i=6}^{N-1}\langle M_1^{(i-1)}M_0^{(i)}M_1^{(i+1)}\rangle \leq N+2, \end{aligned} \tag{C.4}$$

with a corresponding quantum violation of $\beta^{(2)}_Q = N-6+8\sqrt{2}$. Let us then notice that we can repeat our trick for all vertices $3i+1$ for $i=1,\ldots,\lfloor N/3\rfloor$ as each pair of them does not belong to each others' neighbourhoods nor shares a common vertex (see Figure C.1 for a pictorial representation). Thus we can generate a series of $\lfloor N/3\rfloor$ Bell inequalities whose classical and quantum values can easily be computed and are given by

$$\beta^C_k = N+k, \qquad \beta^Q_k = N+(4\sqrt{2}-3)k \tag{C.5}$$

with $k=1,\ldots,\lfloor N/3\rfloor$. The sequence satisfies $\beta^Q_{k+1}/\beta^C_{k+1} > \beta^Q_k/\beta^C_k$ for any k and the ratio attains its maximal value for $N=3L$, $k=L$, amounting to exactly $\beta^Q_N/\beta^C_N = \sqrt{2}$. The resulting inequality read as follows

$$\begin{aligned} I^{\max}_{\text{ring}} \;:=\; & \sum_{i=1}^{L} 2\langle M_1^{(3i)}(M_0^{(3i+1)}+M_1^{(3i+1)})M_1^{(3i+2)}\rangle \\ & + \langle (M_0^{(3i+1)}-M_1^{(3i+1)})M_0^{(3i+2)}M_1^{(3i+3)}\rangle \\ & + \langle M_1^{(3i-1)}M_0^{(3i)}(M_0^{(3i+1)}-M_1^{(3i+1)})\rangle. \end{aligned} \tag{C.6}$$

C.2 Proof of the self-testing statement for graph states

In this section we provide the proof of Fact 3. Before proving this fact, we need some preparation. Let us consider a graph G and the corresponding graph state $|\psi_G\rangle$. Let us also assume that the Bell inequality (5.4) associated to this graph is maximally violated by a state $|\psi\rangle$ and observables $\bar{M}^{(i)}_j$. We then consider the following operators

$$\mathbb{X}'_1 = \frac{1}{\sqrt{2}}\left(\bar{M}_0^{(1)}+\bar{M}_1^{(1)}\right), \quad \mathbb{Z}'_1 = \frac{1}{\sqrt{2}}\left(\bar{M}_0^{(1)}-\bar{M}_1^{(1)}\right), \tag{C.7}$$

and $\mathbb{X}_1 = \mathbb{X}'_1/|\mathbb{X}'_1|$ and $\mathbb{Z}_1 = \mathbb{Z}'_1/|\mathbb{Z}'_1|$. We also denote $\mathbb{X}_i = \bar{M}_0^{(i)}$ and $\mathbb{Z}_i = \bar{M}_1^{(i)}$ for $i = 2, \ldots, N$. It is not difficult to check that all the operators $\mathbb{X}_i$ and $\mathbb{Z}_i$ with $i = 1, \ldots, N$ are unitary; for $i = 2, \ldots, N$ this follows from the fact that $M_j^{(i)}$ are Hermitian and have eigenvalues ± 1, whereas for $i = 1$ it stems from the polar decomposition (see, e.g., Ref. [ŠASA16]). Let us finally choose as isometry the so-called SWAP isometry, as defined in Section 2.3.4, whose output reads as follows

$$\Phi\left(|+\rangle^{\otimes N} \otimes |\psi\rangle\right) = \sum_{\tau \in \{0,1\}^N} |\tau\rangle \otimes \left(\bigotimes_{j=1}^{N} \mathbb{X}_j^{\tau_j} \mathbb{Z}_j^{(\tau_j)}\right) |\psi\rangle\,, \tag{C.8}$$

where $\mathbb{X}_i$ and $\mathbb{Z}_i$ are those defined above and we have also defined $\mathbb{Z}_i^{(\tau_j)} = [\mathbb{1} + (-1)^{\tau_j}\mathbb{Z}_j]/2$, while the summation is over all N-element sequences $(\tau_1, \ldots, \tau_N)$ with each $\tau_i \in \{0, 1\}$. Notice that the action of this isometry is to perform a unitary operation $\Phi = \Phi_1 \otimes \ldots \otimes \Phi_N$ on the state $|+\rangle^{\otimes N} \otimes |\psi\rangle$, where each unitary Φ_i acts on the i-th particle of $|\psi\rangle$ and one of the qubits in the state $|+\rangle$. A visual representation of a local branch of the isometry Φ_i is shown in Fig. 2.7.

We are now ready to prove Fact 3.

Proof. For the sake of simplicity let us assume that $2 \in n(1)$ (notice that this can always be done by relabelling the vertices). Let us also notice that, as shown in Ref. [BP15], one has $\mathbb{X}_1 |\psi\rangle = \mathbb{X}'_1 |\psi\rangle$ and $\mathbb{Z}_1 |\psi\rangle = \mathbb{Z}'_1 |\psi\rangle$, and so in what follows we will denote the operators in Eq. (C.7) by $\mathbb{X}_1$ and $\mathbb{Z}_1$, respectively.

The first step of our proof is to show that $\mathbb{X}_1$ and $\mathbb{Z}_1$ as well as $\mathbb{X}_i$ and $\mathbb{Z}_i$ with $i = 2, \ldots, N$ anticommute when acting on $|\psi\rangle$, that is,

$$(\mathbb{X}_i \mathbb{Z}_i + \mathbb{Z}_i \mathbb{X}_i) |\psi\rangle = 0 \qquad (i = 1, \ldots, N). \tag{C.9}$$

To prove that (C.9) holds true for $i = 1$ it suffices to use the definitions (C.7). Then, to prove (C.9) for the rest of vertices, let us first consider the case $i \in n(1)$. For these vertices, the sum of squares decomposition (5.6), implies the following relations

$$\begin{aligned} \mathbb{X}_1 |\psi\rangle &= \bigotimes_{i \in n(1)} \mathbb{Z}_i |\psi\rangle\,, \\ \mathbb{Z}_1 |\psi\rangle &= \mathbb{X}_2 \otimes \left(\bigotimes_{i \in n(m) \setminus \{1\}} \mathbb{Z}_i\right) |\psi\rangle\,, \end{aligned} \tag{C.10}$$

which can equivalently be stated as

$$\mathbb{X}_1 \otimes \left(\bigotimes_{i \in n(1) \setminus \{m\}} \mathbb{Z}_i \right) |\psi\rangle = \mathbb{Z}_m |\psi\rangle , \tag{C.11}$$

$$\mathbb{Z}_1 \otimes \left(\bigotimes_{i \in n(m) \setminus \{1\}} \mathbb{Z}_i \right) |\psi\rangle = \mathbb{X}_m |\psi\rangle , \tag{C.12}$$

where $m \in N(1)$. By plugging Eqs. (C.11) and (C.12) into Eq. (C.9) we have

$$(\mathbb{X}_m \mathbb{Z}_m + \mathbb{Z}_m \mathbb{X}_m) |\psi\rangle = \left[(\mathbb{Z}_1 \mathbb{X}_1 + \mathbb{X}_1 \mathbb{Z}_1) \otimes \bigotimes_{i \in n(1,m)} \mathbb{Z}_i \right] |\psi\rangle = 0 \tag{C.13}$$

where $n(1, m)$ stands for the neighbours of the first and the mth vertex (excluding these two vertices). Due to the fact that, as proven before, $\mathbb{X}_1$ and $\mathbb{Z}_1$ anticommute, the right-hand side of the above relation vanishes which gives us (C.9) for all $i \in n(1)$.

Let us then prove the anticommutation relation (C.9) for all vertices that are not in $n(1)$ but are neighbours of those belonging to $n(1)$. Consider a vertex $j \notin n(1)$, which is a neighbour of a vertex $k \in n(1)$. For it the decomposition (5.6) implies the following relations

$$\mathbb{X}_j |\psi\rangle = \left[\mathbb{Z}_k \otimes \bigotimes_{i \in n(j) \setminus \{k\}} \mathbb{Z}_i \right] |\psi\rangle \tag{C.14}$$

and

$$\mathbb{Z}_j |\psi\rangle = \left[\mathbb{X}_k \otimes \bigotimes_{i \in n(k) \setminus \{j\}} \mathbb{Z}_i \right] |\psi\rangle , \tag{C.15}$$

from which one obtains

$$\begin{aligned} (\mathbb{X}_j \mathbb{Z}_j + \mathbb{Z}_j \mathbb{X}_j) |\psi\rangle &= \left[(\mathbb{Z}_k \mathbb{X}_k + \mathbb{X}_k \mathbb{Z}_k) \otimes \bigotimes_{i \in n(j,k)} \mathbb{Z}_i \right] |\psi\rangle \\ &= 0, \end{aligned} \tag{C.16}$$

where the last equality stems from the anticommutation relation for $\mathbb{X}_k$ and $\mathbb{Z}_k$.

Noting that there are no isolated vertices in the graph, we can repeat the above procedure until (C.9) is proven for all vertices.

Having the anticommutation relations (C.9) for all vertices of the graph, the remainder of the proof is exactly the same as that of Theorem 4 in Ref. [ŠCAA18] (see Appendix F therein). However, for completeness we present it here.

Let us go back to the action of the unitary operation $\Phi = \Phi_1 \otimes \ldots \otimes \Phi_N$ on the state $|+\rangle^{\otimes N} \otimes |\psi\rangle$. Let us consider a particular term from output state given in (C.8), corresponding to the sequence τ which has $k > 0$ ones at the positions $j_1, \ldots, j_k$:

$$|\tau\rangle \otimes \left(\bigotimes_{j \notin J(\tau)} \mathbb{Z}_j^{(0)} \right) \otimes \left(\bigotimes_{j \in J(\tau)} \mathbb{X}_j \mathbb{Z}_j^{(1)} \right) |\psi\rangle \,, \tag{C.17}$$

where $J(\tau) = \{j_1, \ldots, j_k\}$. Also, for τ let us denote by $n(\tau)$ the number of edges connecting vertices denoted by labels $j \in J(\tau)$ (without counting the same edge twice). Consider then one of the vertices from $J(\tau)$, denoted by j_1, and let the number of its neighbours in $J(\tau)$ be $\bar{n}(j_1)$, i.e., $\bar{n}(j_1) = |J(\tau) \cap n(j_1)|$. Due to the anticommutation relation $\{\mathbb{X}_{j_1}, \mathbb{Z}_{j_1}\} |\psi\rangle = 0$, the expression (C.17) can be rewritten as

$$\begin{aligned} |\tau\rangle \otimes \left(\bigotimes_{j \notin J(\tau)} \mathbb{Z}_j^{(0)} \right) \otimes \left(\bigotimes_{j \in J(\tau) \setminus \{j_1\}} \mathbb{X}_j \mathbb{Z}_j^{(1)} \right) \otimes \mathbb{X}_{j_1} \mathbb{Z}_{j_1}^{(1)} |\psi\rangle \\ = (-1)^{\bar{n}(j_1)} |\tau\rangle \otimes \left(\bigotimes_{j \notin J(\tau)} \mathbb{Z}_j^{(0)} \right) \\ \otimes \left(\bigotimes_{j \in J(\tau) \setminus \{j_1\}} \mathbb{X}_j \mathbb{Z}_j^{(1)} \right) \otimes \mathbb{Z}_{j_1}^{(0)} |\psi\rangle \,, \end{aligned} \tag{C.18}$$

where we have also used the following relation

$$\mathbb{X}_i |\psi\rangle = \bigotimes_{j \in N(i)} \mathbb{Z}_j |\psi\rangle \,, \tag{C.19}$$

that stems from the sum of squares decomposition (5.6) and the fact that $\mathbb{Z}_j^{(1)} \mathbb{Z}_j = -\mathbb{Z}_j^{(1)}$. By using the anticommutation relations (C.9) as well as the relations (C.14), in a similar way we can get rid of all the operators $\mathbb{X}_j$ appearing in (C.17). This allows us to rewrite (C.17) as

$$(-1)^{n(\tau)} |\tau\rangle \otimes \left(\bigotimes_{j=1}^{N} \mathbb{Z}_j^{(0)} \right) |\psi\rangle \,. \tag{C.20}$$

After plugging the above into Eq. (C.8), one obtains

$$\begin{aligned}
&\Phi\left(|+\rangle^{\otimes N}\otimes|\psi\rangle\right) = \\
&= \sum_{\tau\in\{0,1\}^N}(-1)^{n(\tau)}\,|\tau\rangle\otimes\left(\bigotimes_{j=1}^{N}\mathbb{Z}_j^{(0)}\right)|\psi\rangle \\
&= |\psi_G\rangle\otimes|\mathrm{aux}\rangle\,,
\end{aligned} \tag{C.21}$$

where we used the expression for a graph state in the computational basis

$$|\psi_G\rangle = \frac{1}{\sqrt{2}^N}\sum_{\tau\in\{0,1\}^N}(-1)^{n(\tau)}\,|\tau\rangle\,.$$

This completes the proof. The proof for self-testing of measurements goes along the same lines as the one for the state (see for example Appendix E of [ŠCAA18]). □

C.3 Self-testing the partially entangled GHZ state from its stabilizers

Here we look at the method used to derive Bell inequalities for graph states as a more general strategy, so to apply it to other states as well. We will show how to do it for the partially entangled GHZ state (5.26). Recall that for this state it is possible to define N independent stabilizing operators:

$$G_1 = \sin 2\theta X_1X_2\ldots X_N + \cos 2\theta Z_1 \tag{C.22}$$

for the first site, and

$$G_i = Z_1Z_i \tag{C.23}$$

for sites $i = 2,\ldots,N$. Indeed, one can verify that $G_i|\mathrm{GHZ}_N(\theta)\rangle = |\mathrm{GHZ}_N(\theta)\rangle$ for any $\theta\in[0,\pi/4]$ and $i = 1,\ldots,N$.

We will start by showing how to generalise the self-testing method introduced in Appendix C.2 for the graph states and then building on that we will derive Bell inequalities for the partially entangled GHZ states.

Self-testing proof

Let us begin by making the following substitutions

$$\mathbb{X}'_1 = \frac{M_0^{(1)}+M_1^{(1)}}{2\sin\mu}, \qquad \mathbb{Z}'_1 = \frac{M_0^{(1)}-M_1^{(1)}}{2\cos\mu}, \tag{C.24}$$

with their regularized versions being $\mathbb{X}_1 = \mathbb{X}'_1/|\mathbb{X}'_1|$, $\mathbb{Z}_1 = \mathbb{Z}'_1/|\mathbb{Z}'_1|$ and $\mathbb{X}_i = M_0^{(i)}$, $\mathbb{Z}_i = M_1^{(i)}$ for $i = 2,\ldots,N$. Notice that the operators for the

first observer anticommute by construction, while all the remaining ones square to identity, that is, $\mathbb{X}_i^2 = \mathbb{Z}_i^2 = \mathbb{1}$.

Suppose now that we are given a Bell expression $\mathcal{I}$ whose maximal quantum value β_Q is achieved by a state $|\psi\rangle$. Let us assume, moreover, that the corresponding Bell operator $\mathcal{B}$ admits the following sum of squares

$$c(\beta_Q \mathbb{1} - \mathcal{B}) = \sum_{i=1}^{N} \alpha_i^2 (\mathbb{1} - \tilde{G}_i)^2, \tag{C.25}$$

where we identify with $\tilde{G}_i$ the stabilizer operators with the substituted operators $\mathbb{X}_i, \mathbb{Z}_i$ (cfr. Eq. (5.30)). Such a decomposition would imply that the state $|\psi\rangle$ satisfies the stabilizing conditions

$$\tilde{G}_i |\psi\rangle = |\psi\rangle \tag{C.26}$$

with $i = 1, \ldots, N$.

We now proceed to show that, with any choice of operators of the kind of (C.24), the above two equations suffice to self-test the partially entangled GHZ state for any $\theta \in (0, \pi/4]$.

First, let us see how the stabilizing conditions allow to prove that all the pairs $\mathbb{X}_i, \mathbb{Z}_i$ anticommute and square to identity when acting on the state.

Let us begin with $\mathbb{X}_1$ and $\mathbb{Z}_1$. First, from the definitions (C.24) we directly see that

$$\{\mathbb{X}_1, \mathbb{Z}_1\} = 0. \tag{C.27}$$

Then, from the conditions (C.26) and the fact that $\mathbb{Z}_i^2 = \mathbb{1}$ for any $i = 2, \ldots, N$ we immediately obtain $\mathbb{Z}_1 |\psi\rangle = \mathbb{Z}_i |\psi\rangle$, which implies that

$$\mathbb{Z}_1^2 |\psi\rangle = \mathbb{Z}_1 \mathbb{Z}_i |\psi\rangle = \tilde{S}_i |\psi\rangle = |\psi\rangle , \tag{C.28}$$

and, as a result, that $\tilde{G}_i^2 |\psi\rangle = |\psi\rangle$. To finally prove that $\mathbb{X}_i^2 = \mathbb{1}$, we rewrite (C.24) as

$$\mathbb{X}_1 = \frac{1}{\sin 2\theta} (\tilde{G}_1 - \cos 2\theta \mathbb{Z}_1) \mathsf{X}_1, \tag{C.29}$$

where $\mathsf{X}_1 = \mathbb{X}_2 \ldots \mathbb{X}_N$. Due to the fact that $\mathsf{X}_1^2 = \mathbb{1}$, we then have

$$\mathbb{X}_1^2 = \frac{1}{\sin^2 2\theta} \left[\tilde{G}_1^2 - \cos 2\theta \{\tilde{G}_1, \mathbb{Z}_1\} + \cos^2 2\theta \mathbb{Z}_1^2 \right]. \tag{C.30}$$

From the very definition of $\tilde{G}_1$ we can rewrite the anticommutator appearing in the above as

$$\begin{aligned} \{\tilde{G}_1, \mathbb{Z}_1\} &= \sin 2\theta \{\mathbb{X}_1, \mathbb{Z}_1\} \mathsf{X}_1 + 2 \cos 2\theta \mathbb{Z}_1^2 \\ &= 2 \cos 2\theta \mathbb{Z}_1^2, \end{aligned} \tag{C.31}$$

where the second equality stems from the anticommutation relation (C.27). The identity (C.31) allows us to simplify Eq. (C.30) as

$$\mathbb{X}_1^2 = \frac{1}{\sin^2 2\theta}\left(\tilde{G}_1^2 - \cos^2 2\theta \mathbb{Z}_1^2\right), \tag{C.32}$$

which, due to the fact that $\tilde{G}_1^2 |\psi\rangle = \mathbb{Z}_1^2 |\psi\rangle = |\psi\rangle$, directly implies that $\mathbb{X}_1^2 |\psi\rangle = |\psi\rangle$.

Let us now turn to the operators $\mathbb{X}_i$ and $\mathbb{Z}_i$ for the remaining sites $i = 2, \ldots, N$. We have already noticed that $\mathbb{X}_i^2 = \mathbb{Z}_i^2 = \mathbb{1}$, so in what follows we prove that they anticommute. With the aid of Eq. (C.22) we can express $\mathbb{X}_i$ as

$$\mathbb{X}_i = \frac{1}{\sin 2\theta}\mathsf{X}_i\left(\tilde{G}_1 - \cos 2\theta \mathbb{Z}_1\right), \tag{C.33}$$

where $\mathsf{X}_i = \mathbb{X}_1 \ldots \mathbb{X}_{i-1}\mathbb{X}_{i+1} \ldots \mathbb{X}_N$. This, after some straightforward manoeuvres, allows us to write

$$\{\mathbb{X}_i, \mathbb{Z}_i\} |\psi\rangle = \frac{1}{\sin 2\theta}\mathsf{X}_i\left[\{\tilde{S}_1, \mathbb{Z}_1\} - 2\cos 2\theta \mathbb{Z}_1^2\right] |\psi\rangle \tag{C.34}$$

To see that the right-hand side of the above equation vanishes it suffices to use Eq. (C.31).

We have thus established that

$$\{\mathbb{X}_i, \mathbb{Z}_i\} |\psi\rangle = 0 \tag{C.35}$$

as well as $dix_i^2 |\psi\rangle = diz_i^2 |\psi\rangle = |\psi\rangle$ for all $i = 1, \ldots, N$. Let us now use them to prove our self-testing statement with the isometry $\Phi = \Phi_1 \otimes \ldots \otimes \Phi_N$ with each Φ_i traditionally defined as in Fig. 5.1. As above, each operator Φ_i acts on one of the particles of state $|\psi\rangle$ and a qubit state $|+\rangle$, giving

$$\Phi\left(|+\rangle^{\otimes N} \otimes |\psi\rangle\right) = \sum_{\tau \in \{0,1\}^N} |\tau\rangle \otimes \left(\bigotimes_{j=1}^{N} \mathbb{X}_j^{\tau_j} \mathbb{Z}_j^{(\tau_j)}\right) |\psi\rangle, \tag{C.36}$$

Let us first show that all terms in (C.36) except for $\tau = (0, \ldots, 0)$ and $\tau = (1, \ldots, 1)$ vanish. To this end, consider a sequence τ in which $\tau_m = 0$ and $\tau_n = 1$ for some $m \neq n$. For such a sequence we can rewrite the corresponding term in (C.36) as

$$\begin{aligned} &\left(\bigotimes_{j \neq m,n} \mathbb{X}_j^{\tau_j} \mathbb{Z}_j^{(\tau_j)}\right) \otimes \mathbb{Z}_m^{(0)} \mathbb{X}_n \mathbb{Z}_n^{(1)} |\psi\rangle \\ &= \left(\bigotimes_{j \neq j_1, j_2} \mathbb{X}_j^{\tau_j} \mathbb{Z}_j^{(\tau_j)}\right) \otimes \mathbb{X}_n \mathbb{Z}_1^{(1)} \mathbb{Z}_1^{(0)} |\psi\rangle, \end{aligned} \tag{C.37}$$

where we used the anticommutation relation for $\mathbb{X}_n$ and $\mathbb{Z}_n$ as well as the fact that $\mathbb{Z}_i |\psi\rangle = \mathbb{Z}_1 |\psi\rangle$ for $i = 2, \ldots, N$. Noticing then that $\mathbb{Z}_1^{(1)}\mathbb{Z}_1^{(0)} = 0$ as both $\mathbb{Z}_1^{(i)}$ are unnormalised projections onto orthogonal subspaces, we see that (C.37) amounts to zero.

Hence, the expression (C.36) reduces to the following two terms

$$\begin{aligned}
&\Phi\left(|+\rangle^{\otimes N} \otimes |\psi\rangle\right) = |0\rangle^{\otimes N} \otimes \left(\mathbb{Z}_1^{(0)} \ldots \mathbb{Z}_N^{(0)}\right) |\psi\rangle \\
&+ |1\rangle^{\otimes N} \otimes \left(\mathbb{X}_1\mathbb{Z}_1^{-} \ldots \mathbb{X}_N\mathbb{Z}_N^{-}\right) |\psi\rangle \\
&= |0\rangle^{\otimes N} \otimes (\mathbb{Z}_1^{(0)})^N |\psi\rangle + |1\rangle^{\otimes N} \otimes \left[\mathbb{X}_1(\mathbb{Z}_1^{(1)})^N\mathbb{X}_2 \ldots \mathbb{X}_N\right] |\psi\rangle \\
&= |0\rangle^{\otimes N} \otimes \mathbb{Z}_1^{(0)} |\psi\rangle + |1\rangle^{\otimes N} \otimes \left[\mathbb{Z}_1^{(0)}\mathbb{X}_1 \ldots \mathbb{X}_N\right] |\psi\rangle\,, \qquad \text{(C.38)}
\end{aligned}$$

where to obtain the second equality we exploited conditions (C.26) for all $i = 2, \ldots, N$, whereas the second equality follows from the fact that $[\mathbb{Z}_1^{(j)}]^2 |\psi\rangle = \mathbb{Z}_1^{(j)} |\psi\rangle$ for $j = 0, 1$ and the anticommutation relation (C.27). Using then (C.22), the above can be rewritten as

$$\begin{aligned}
\Phi\left(|+\rangle^{\otimes N} \otimes |\psi\rangle\right) &= \frac{1}{\sin 2\theta}\Big[\sin 2\theta\, |0\rangle^{\otimes N} \otimes \mathbb{Z}_1^{(0)} |\psi\rangle \\
&\quad + |1\rangle^{\otimes N} \otimes (\mathbb{Z}_1^{(0)}\tilde{G}_1 - \cos 2\theta\mathbb{Z}_1^{(0)}\mathbb{Z}_1) |\psi\rangle\Big] \\
&= \frac{1}{\sin 2\theta}\left[\sin 2\theta\, |0\rangle^{\otimes N} + (1 - \cos 2\theta)\, |1\rangle^{\otimes N}\right] \otimes \mathbb{Z}_1^{(0)} |\psi\rangle \\
&= |\mathrm{aux}\rangle \otimes |\mathrm{GHZ}_N(\theta)\rangle\,, \qquad \text{(C.39)}
\end{aligned}$$

where $|\mathrm{aux}\rangle = (1/\cos\theta)\mathbb{Z}_1^{(0)} |\psi\rangle$. To obtain the second equality we used the facts that $\tilde{G}_1$ stabilizes $|\psi\rangle$ and that $\mathbb{Z}_1^{(0)}\mathbb{Z}_1 = \mathbb{Z}_1^{(0)}$, while the last one is a consequence of the two well-known trigonometric relations $\sin 2\theta = 2\sin\theta\cos\theta$ and $1 - \cos 2\theta = 2\sin^2\theta$. This completes our self-testing statement.

Deriving the Bell inequality

Notice how the previous self-testing argument justifies the choice (C.25) for a SOS decomposition. Now, what is left to show is that (C.25) (cfr. Eq. (5.30)) can indeed be satisfied and thus give rise to a non-trivial Bell inequality. We see that this can be done by choosing the free angle μ and the α_i parameters accordingly. To do so, let us first compute the square of the stabilizing operators

$$\begin{aligned}
\tilde{G}_1^2 &= \frac{1}{2}\left(\frac{\sin^2 2\theta}{\sin^2\mu} + \frac{\cos^2 2\theta}{\cos^2\mu}\right)\mathbb{1} \\
&\quad + \frac{1}{4}\left(\frac{\sin^2 2\theta}{\sin^2\mu} - \frac{\cos^2 2\theta}{\cos^2\mu}\right)\{M_0^{(1)}, M_1^{(1)}\} \qquad \text{(C.40)}
\end{aligned}$$

and

$$\tilde{G}_i^2 = \frac{1}{2\cos^2\mu}\mathbb{1} - \frac{1}{4\cos^2\mu}\{M_0^{(1)}, M_1^{(1)}\} \tag{C.41}$$

for $i = 2, \ldots, N$. With these identities the sum of squares (C.25) can be expanded as

$$\begin{aligned}\sum_{i=1}^{N}\alpha_i^2(\mathbb{1}-\tilde{G}_i)^2 &= \sum_{i=1}^{N}\alpha_i^2\mathbb{1} - 2\sum_{i=1}^{N}\alpha_i^2\tilde{G}_i \\ &+\frac{1}{2}\left[\left(\frac{\sin^2 2\theta}{\sin^2\mu}+\frac{\cos^2 2\theta}{\cos^2\mu}\right)\alpha_1^2 + \frac{1}{\cos^2\mu}\sum_{i=2}^{N}\alpha_i^2\right]\mathbb{1} \\ &+\frac{1}{4}\left[\left(\frac{\sin^2 2\theta}{\sin^2\mu}-\frac{\cos^2 2\theta}{\cos^2\mu}\right)\alpha_1^2 - \frac{1}{\cos^2\mu}\sum_{i=2}^{N}\alpha_i^2\right]\{M_0^{(1)}, M_1^{(1)}\}\end{aligned} \tag{C.42}$$

Now, we want the term standing in front of the anticommutator to vanish. This can be done by setting: $\alpha_1^2 = \sqrt{2}(N-1)$ and $\alpha_2^2 = \ldots = \alpha_N^2 = \sqrt{2}$ and the angle μ so that $2\sin^2\mu = \sin^2 2\theta$. This gives

$$\sum_{i=1}^{N}\alpha_i^2(\mathbb{1}-\tilde{G}_i)^2 = 2\left\{2\sqrt{2}(N-1)\mathbb{1} - \left[(N-1)\sqrt{2}\tilde{G}_1 + \sqrt{2}\sum_{i=2}^{N}\tilde{G}_i\right]\right\}, \tag{C.43}$$

where we keep the $\sqrt{2}$ factor inside the curly brackets for further convenience. We can thus identify $\beta_Q = 2\sqrt{2}(N-1)$ and the remaining terms appearing on the left-hand side of the above as the Bell operator

$$\mathcal{B} = (N-1)\sqrt{2}\tilde{G}_1 + \sqrt{2}\sum_{i=2}^{N}\tilde{G}_i. \tag{C.44}$$

This, after substituting the expressions of the operators $\mathbb{X}_i, \mathbb{Z}_i$ in terms of arbitrary observables for all i, leads us to the following Bell inequality

$$\begin{aligned}\mathcal{I}_\theta \;:=\; & (N-1)\langle(M_0^{(1)}+M_1^{(1)})M_0^{(2)}\ldots M_0^{(N)}\rangle \\ & +(N-1)\frac{\cos 2\theta}{\sqrt{1+\cos^2 2\theta}}(\langle M_0^{(1)}\rangle - \langle M_1^{(1)}\rangle) \\ & +\frac{1}{\sqrt{1+\cos^2 2\theta}}\sum_{i=2}^{N}\langle(M_0^{(1)}-M_1^{(1)})M_1^{(i)}\rangle \leq \beta_C,\end{aligned} \tag{C.45}$$

where β_C is the classical bound that we compute below. For this purpose, we can optimize $\mathcal{I}_\theta$ over all the deterministic strategies corresponding to the different choices $M_{x_i}^{(i)} = \pm 1$. Given the simple form of the inequality, we can divide into the two subcases $M_0^{(1)} = \pm M_1^{(1)}$ and notice that the

maximum is attained in the case in which the observables of the first party take opposite signs, which results in

$$\beta_C(\theta) = 2(N-1)\frac{1+\cos 2\theta}{\sqrt{1+\cos^2 2\theta}}. \tag{C.46}$$

Notice that $\beta_C(\pi/4) = 2(N-1)$ and we recover the limit case of the GHZ state and inequality (5.14), while for $\theta = 0$ one has $\beta_C(0) = 2\sqrt{2}(N-1)$ and there is obviously no quantum violation. Moreover one can see that $\beta_C(\theta)$ is a decreasing function of θ in the considered interval. This implies that (C.45) is violated for any value of θ in the given interval. Interestingly, in the case $N = 2$ we obtain a self-testing inequality for the partially entangled two-qubit state that is inequivalent to the known tilted CHSH [AMP12, BP15] .

Bibliography

[ABB+10] M. L. Almeida, J.-D. Bancal, N. Brunner, A. Acín, N. Gisin, and S. Pironio. Guess your neighbor's input: A multipartite nonlocal game with no quantum advantage. *Physical Review Letters*, 104:230404, 2010.

[ABG+07] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98:230501, 2007.

[ADR82] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49:1804–1807, 1982.

[AIIS04] D. Avis, H. Imai, T. Ito, and Y. Sasaki. Deriving tight Bell inequalities for 2 parties with many 2-valued observables from facets of cut polytopes. *arXiv preprint quant-ph/0404014*, 2004.

[AKGT17] I. Apellaniz, M. Kleinmann, O. Gühne, and G. Tóth. Optimal witnessing of the quantum Fisher information with few measurements. *Physical Review A*, 95:032330, 2017.

[AMP12] A. Acín, S. Massar, and S. Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108:100402, 2012.

[Avi00] D. Avis. A revised implementation of the reverse search vertex enumeration algorithm. In *Polytopes–combinatorics and computation*, pages 177–198. Springer, 2000.

[Bar82] F. Barahona. On the computational complexity of Ising spin glass models. *Journal of Physics A: Mathematical and General*, 15(10):3241–3253, 1982.

[BAŠ+18] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín. Scalable Bell inequalities for qubit graph states and robust self-testing. *arXiv preprint arXiv:1812.10428*, 2018.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore*, 1984.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[BBD+09] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, 2009.

[BBGL11] J.-D. Bancal, N. Brunner, N. Gisin, and Y.-C. Liang. Detecting genuine multipartite quantum nonlocality: A simple approach and generalization to arbitrary dimensions. *Physical Review Letters*, 106:020405, 2011.

[BBGP09] J.-D. Bancal, C. Branciard, N. Gisin, and S. Pironio. Quantifying multipartite nonlocality. *Physical Review Letters*, 103:090503, 2009.

[BBGP13] J.-D. Bancal, J. Barrett, N. Gisin, and S. Pironio. Definitions of multipartite nonlocality. *Physical Review A*, 88:014102, 2013.

[BBS+13] J. T. Barreiro, J.-D. Bancal, P. Schindler, D. Nigg, M. Hennrich, T. Monz, N. Gisin, and R. Blatt. Demonstration of genuine multipartite entanglement with device-independent witnesses. *Nature Physics*, 9(9):559, 2013.

[BC12] F. G. S. L. Brandão and M. Christandl. Detection of multiparticle entanglement: Quantifying the search for symmetric extensions. *Physical Review Letters*, 109(16):160502, 2012.

[BCP+14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[BCWA17] F. Baccari, D. Cavalcanti, P. Wittek, and A. Acín. Efficient device-independent entanglement detection for multipartite systems. *Physical Review X*, 7:021042, 2017.

[BD94] M. R. Bhatt and U. B. Desai. Robust image restoration algorithm using markov random field model. *CVGIP: Graphical Models and Image Processing*, 56(1):61–74, 1994.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[BFL91] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational complexity*, 1(1):3–40, 1991.

[BGLP11] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio. Device-independent witnesses of genuine multipartite entanglement. *Physical Review Letters*, 106:250404, 2011.

[BGWA18] F. Baccari, C. Gogolin, P. Wittek, and A. Acín. Verification of quantum optimizers. *arXiv preprint arXiv:1808.01275*, 2018.

[BHJ+14] P. I. Bunyk, E. M. Hoskinson, M. W. Johnson, E. Tolkacheva, F. Altomare, A. J. Berkley, R. Harris, J. P. Hilton, T. Lanting, A. J. Przybysz, et al. Architectural considerations in the design of a superconducting quantum annealing processor. *IEEE Transactions on Applied Superconductivity*, 24(4):1–10, 2014.

[BLM+05] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Nonlocal correlations as an information-theoretic resource. *Physical Review A*, 71:022101, 2005.

[BP05] J. Barrett and S. Pironio. Popescu-Rohrlich correlations as a unit of nonlocality. *Physical Review Letters*, 95:140401, 2005.

[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. *Physical Review A*, 91:052111, 2015.

[BPA+08] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Méthot, and V. Scarani. Testing the dimension of Hilbert spaces. *Physical Review Letters*, 100:210503, 2008.

[Bre06] H.-P. Breuer. Optimal entanglement criterion for mixed quantum states. *Physical Review Letters*, 97:080501, 2006.

[BŠCA18a] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín. Device-independent entanglement certification of all entangled states. *arXiv preprint arXiv:1801.10444*, 2018.

[BŠCA18b] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín. Self-testing of Pauli observables for device-independent entanglement certification. *arXiv preprint arXiv:1801.10446*, 2018.

[BTF+18] F. Baccari, J. Tura, M. Fadel, A. Aloy, J.-D. Bancal, N. Sangouard, M. Lewenstein, A. Acín, and R. Augusiak. Bell correlations depth in many-body systems. *arXiv preprint arXiv:1802.09516*, 2018.

[BV04] S. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[BW92] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69:2881–2884, 1992.

[CG04] D. Collins and N. Gisin. A relevant two qubit Bell inequality inequivalent to the CHSH inequality. *Journal of Physics A: Mathematical and General*, 37(5):1775, 2004.

[CGL15] F. J. Curchod, N. Gisin, and Y.-C. Liang. Quantifying multipartite nonlocality via the size of the resource. *Physical Review A*, 91:012121, 2015.

[CGS17] A. Coladangelo, K. T. Goh, and V. Scarani. All pure bipartite entangled states can be self-tested. *Nature communications*, 8:15485, 2017.

[CH16] E. Crosson and A. W. Harrow. Simulated quantum annealing can be exponentially faster than classical simulated annealing. In *2016 IEEE 57th Annu. Symp. Found. Comput. Sci.*, volume 2016-Decem, pages 714–723. IEEE, 2016.

[Cha93] B. Chazelle. An optimal convex hull algorithm in any fixed dimension. *Discrete & Computational Geometry*, 10(4):377–409, 1993.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

[CK07] D. Chruściński and A. Kossakowski. On the structure of entanglement witnesses and new class of positive indecomposable maps. *Open Systems and Information Dynamics*, 14(3):275–294, 2007.

[CLY+17] L.-K. Chen, Z.-D. Li, X.-C. Yao, M. Huang, W. Li, H. Lu, X. Yuan, Y.-B. Zhang, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, X. Ma, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan. Observation of ten-photon entanglement using thin BiB3O6 crystals. *Optica*, 4(1):77–83, 2017.

[Cro18] G. E. Crooks. Performance of the quantum approximate optimization algorithm on the maximum cut problem. *arxiv preprint arxiv:1811.08419*, 2018.

[CS17] D. Cavalcanti and P. Skrzypczyk. Quantum steering: a review with focus on semidefinite programming. *Reports on Progress in Physics*, 80(2):024001, 2017.

[Cvx] M. Grant and S. Boyd. http://cvxr.com/cvx/.

[CW03] K. Chen and L. Wu. A matrix realignment method for recognizing entanglement. *Quantum Information & Computation*, 3(3):193–202, 2003.

[DBI+16] V. S. Denchev, S. Boixo, S. V. Isakov, N. Ding, R. Babbush, V. Smelyanskiy, J. Martinis, and H. Neven. What is the computational value of finite range tunneling? *Physical Review X*, 6(3):031015, 2016.

[Dic54] R. H. Dicke. Coherence in spontaneous radiation processes. *Physical Review*, 93(1):99, 1954.

[DLTW08] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner. The quantum moment problem and bounds on entangled multi-prover games. *Proc. IEEE 23rd Annual Conf. Comp. Compl.*, pages 199–210, 2008.

[DPS02] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Distinguishing separable and entangled states. *Physical Review Letters*, 88:187904, 2002.

[DPS04] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Complete family of separability criteria. *Physical Review A*, 69:022308, 2004.

[DPS05] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Detecting multipartite entanglement. *Physical Review A*, 71(3):032333, 2005.

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.

[EKHK17] N. J. Engelsen, R. Krishnakumar, O. Hosten, and M. A. Kasevich. Bell correlations in spin-squeezed states of 500 000 atoms. *Physical Review Letters*, 118:140401, 2017.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[ERIR+08] K. Eckert, O. Romero-Isart, M. Rodriguez, M. Lewenstein, E. S. Polzik, and A. Sanpera. Quantum non-demolition detection of strongly correlated systems. *Nature Physics*, 4(1):50, 2008.

[FC72] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28:938–941, 1972.

[FGG14] E. Farhi, J. Goldstone, and S. Gutmann. A Quantum Approximate Optimization Algorithm. Technical report, MIT, 2014.

[Fin82] A. Fine. Hidden variables, joint probability, and the Bell inequalities. *Physical Review Letters*, 48:291–295, 1982.

[FMM+18] N. Friis, O. Marty, C. Maier, C. Hempel, M. Holzäpfel, P. Jurcevic, M. B. Plenio, M. Huber, C. Roos, R. Blatt, and B. Lanyon. Observation of entangled states of a fully controlled 20-qubit system. *Physical Review X*, 8:021012, 2018.

[Fri12] T. Fritz. Polyhedral duality in Bell scenarios with two binary observables. *Journal of Mathematical Physics*, 53(7):072202, 2012.

[Fuk97] K. Fukuda. cdd/cdd+ reference manual. *Institute for Operations Research, ETH-Zentrum*, pages 91–111, 1997.

[GBB08] O. Gühne, F. Bodoky, and M. Blaauboer. Multiparticle entanglement under the influence of decoherence. *Physical Review A*, 78:060301, 2008.

[GC08] O. Gühne and A. Cabello. Generalized Ardehali-Bell inequalities for graph states. *Physical Review A*, 77:032108, 2008.

[GGH+14] J. Gondzio, J. A. Gruca, J. J. Hall, W. Laskowski, and M. Żukowski. Solving large-scale optimization problems related to Bell's theorem. *Journal of Computational and Applied Mathematics*, 263:392–404, 2014.

[Gha08] S. Gharibian. Strong NP-hardness of the quantum separability problem. *arXiv preprint arXiv:0810.4507*, 2008.

[GHB+02] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. Detection of entanglement with few local measurements. *Physical Review A*, 66(6):062305, 2002.

[GHG10] O. Gittsovich, P. Hyllus, and O. Gühne. Multiparticle covariance matrices and the impossibility of detecting graph-state entanglement with two-particle correlations. *Physical Review A*, 82:032306, 2010.

[GHZ89] D. M. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond Bell's theorem. In *Bell's theorem, quantum theory and conceptions of the universe*, pages 69–72. Springer, 1989.

[GJR87] M. Grötschel, M. Jünger, and G. Reinelt. Calculating exact ground states of spin glasses: A polyhedral approach. In *Heidelberg Colloquium on Glassy Dynamics*, volume 275, pages 325–353. Springer, 1987.

[GKW+18] K. T. Goh, J. m. k. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani. Geome-

try of the set of quantum correlations. *Physical Review A*, 97:022104, 2018.

[GLM04] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–6, 2004.

[Got96] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A*, 54:1862–1868, 1996.

[GS10] O. Gühne and M. Seevinck. Separability criteria for genuine multiparticle entanglement. *New Journal of Physics*, 12(5):053002, 2010.

[GT09] O. Gühne and G. Tóth. Entanglement detection. *Physics Reports*, 474(1-6):1–75, 2009.

[GTHB05] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel. Bell inequalities for graph states. *Physical Review Letters*, 95:120405, 2005.

[Gur03] L. Gurvits. Classical deterministic complexity of edmonds' problem and quantum entanglement. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 10–19. ACM, 2003.

[GVW+15] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. 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. *Physical Review Letters*, 115:250401, 2015.

[GWAN12] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués. Operational framework for nonlocality. *Physical Review Letters*, 109:070401, 2012.

[HBcvB99] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Physical Review A*, 59:1829–1834, 1999.

[HBD+15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N.

Schouten, C. Abellán, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682, 2015.

[HEB04] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Physical Review A*, 69(6):062311, 2004.

[HH99] M. Horodecki and P. Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Physical Review A*, 59:4206–4216, 1999.

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1):1 – 8, 1996.

[HHH01] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps. *Physics Letters A*, 283(1-2):1–7, 2001.

[HHR+05] H. Häffner, W. Hänsel, C. Roos, J. Benhelm, M. Chwalla, T. Körber, U. Rapol, M. Riebe, P. Schmidt, C. Becher, et al. Scalable multiparticle entanglement of trapped ions. *Nature*, 438(7068):643, 2005.

[HSP10] K. Hammerer, A. S. Sørensen, and E. S. Polzik. Quantum interface between light and atomic ensembles. *Reviews Modern Physics*, 82:1041–1093, 2010.

[JM05] N. S. Jones and L. Masanes. Interconversion of nonlocal correlations. *Physical Review A*, 72:052312, 2005.

[JMG11] B. Jungnitsch, T. Moroder, and O. Gühne. Taming multiparticle entanglement. *Physical Review Letters*, 106:190502, 2011.

[Kan16] J. Kaniewski. Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities. *Physical Review Letters*, 117:070402, 2016.

[Kar84] N. Karmarkar. A new polynomial-time algorithm for linear programming. In *Proceedings of the sixteenth annual ACM symposium on Theory of computing*, pages 302–311. ACM, 1984.

[KFGT07] D. Koller, N. Friedman, L. Getoor, and B. Taskar. Graphical models in a nutshell. In *Introduction to Statistical Relational Learning*. MIT Press, 2007.

[KGanidZ+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. *Physical Review Letters*, 85:4418–4421, 2000.

[KGV83] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi. Optimization by Simulated Annealing. *Science*, 220(4598):671–680, 1983.

[KSC+15] I. Kogias, P. Skrzypczyk, D. Cavalcanti, A. Acín, and G. Adesso. Hierarchy of steering criteria based on moments for all bipartite quantum systems. *Physical Review Letters*, 115(21):210401, 2015.

[KSK+16] L. Knips, C. Schwemmer, N. Klein, M. Wieśniak, and H. Weinfurter. Multipartite entanglement detection with minimal effort. *Physical Review Letters*, 117:210504, 2016.

[KST+07] N. Kiesel, C. Schmid, G. Tóth, E. Solano, and H. Weinfurter. Experimental observation of four-photon entangled dicke state with high fidelity. *Physical Review Letters*, 98:063604, 2007.

[KŠT+18] 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 preprint arXiv:1807.03332*, 2018.

[Las01a] J. B. Lasserre. An explicit exact SDP relaxation for nonlinear 0-1 programs. In *International Conference on Integer Programming and Combinatorial Optimization*, pages 293–303. Springer, 2001.

[Las01b] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on optimization*, 11(3):796–817, 2001.

[Las06] J. B. Lasserre. Convergent SDP-relaxations in polynomial optimization with sparsity. *SIAM Journal on optimization*, 17(3):822–843, 2006.

[LJRR04] F. Liers, M. Jünger, G. Reinelt, and G. Rinaldi. Computing exact ground states of hard ising spin glass problems by branch-and-cut. *New optimization algorithms in physics*, 50(47-68):6, 2004.

[LPS+14] T. Lanting, A. J. Przybysz, A. Y. Smirnov, F. M. Spedalieri, M. H. Amin, A. J. Berkley, R. Harris, F. Altomare, S. Boixo, P. Bunyk, N. Dickson, C. Enderud, J. P. Hilton, E. Hoskinson, M. W. Johnson, E. Ladizinsky, N. Ladizinsky, R. Neufeld, T. Oh, I. Perminov, C. Rich, M. C. Thom, E. Tolkacheva, S. Uchaikin, A. B. Wilson, and G. Rose. Entanglement in a quantum annealing processor. *Physical Review X*, 4(2):021041, 2014.

[LPV+14] B. Lücke, J. Peise, G. Vitagliano, J. Arlt, L. Santos, G. Tóth, and C. Klempt. Detecting multiparticle entanglement of Dicke states. *Physical Review Letters*, 112:155304, 2014.

[LRB+15] Y.-C. Liang, D. Rosset, J.-D. Bancal, G. Pütz, T. J. Barnea, and N. Gisin. Family of Bell-like inequalities as device-independent witnesses for entanglement depth. *Physical Review Letters*, 114:190401, 2015.

[Luc14] A. Lucas. Ising formulations of many NP problems. *Frontiers of Physics*, 2:1–15, 2014.

[LZG+07] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan. Experimental entanglement of six photons in graph states. *Nature physics*, 3(2):91, 2007.

[LZJ+14] B. P. Lanyon, M. Zwerger, P. Jurcevic, C. Hempel, W. Dür, H. J. Briegel, R. Blatt, and C. F. Roos. Experimental violation of multipartite Bell inequalities with trapped ions. *Physical Review Letters*, 112:100403, 2014.

[MBL+13] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne. Device-independent entanglement quantification and related applications. *Physical Review Letters*, 111:030501, 2013.

[McK11] M. McKague. Self-testing graph states. In *Conference on Quantum Computation, Communication, and Cryptography*, pages 104–120. Springer, 2011.

[Mer90] N. D. Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65:3373–3376, 1990.

[MK18] S. Mandrá and H. G. Katzgraber. A deceptive step towards quantum speedup detection. *Quantum Science and Technology*, 2018.

[MKT17] S. Mandrá, H. G. Katzgraber, and C. Thomas. The pitfalls of planar spin-glass benchmarks: raising the bar for quantum annealers (again). *Quantum Science and Technology*, 2(3):038501, 2017.

[MMV07] D. Markham, A. Miyake, and S. Virmani. Entanglement and local information access for graph states. *New Journal of Physics*, 9(6):194, 2007.

[Mos] E. D. Andersen and K. D. Andersen. https://www.mosek.com.

[MSB+11] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt. 14-qubit entanglement: Creation and coherence. *Physical Review Letters*, 106:130506, 2011.

[MY04] D. Mayers and A. C. Yao. Self-testing quantum apparatus. *Quantum Information & Computation*, 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.

[NC02] M. A. Nielsen and I. Chuang. Quantum computation and quantum information, 2002.

[NPA07] M. Navascués, S. Pironio, and A. Acín. Bounding the set of quantum correlations. *Physical Review Letters*, 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.

[PAM+10] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021, 2010.

[PBD+00] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger. Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement. *Nature*, 403(6769):515, 2000.

[PBS11] S. Pironio, J.-D. Bancal, and V. Scarani. Extremal correlations of the tripartite no-signaling polytope. *Journal of Physics A: Mathematical and Theoretical*, 44(6):065303, 2011.

[Per96] A. Peres. Separability criterion for density matrices. *Phyical Review Letters*, 77:1413–1415, 1996.

[Pia06] M. Piani. Class of bound entangled states of $n+n$ qubits revealed by nondecomposable maps. *Physical Review A*, 73:012345, 2006.

[Pit89] I. Pitowsky. Quantum probability – quantum logic. *Lecture Notes in Physics, Springer-Verlag Berlin Heidelberg*, 1989.

[PMS+14] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien. A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, 5(1):4213, 2014.

[PNA10] S. Pironio, M. Navascués, and A. Acín. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM Journal on optimization*, 20:2157–2180, 2010.

[PR94] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

[QNN17] QNNCloud. Quantum neural network: Optical neural networks operating at the quantum limit, 2017.

[RB01] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86:5188–5191, 2001.

[RRW08] F. Rendl, G. Rinaldi, and A. Wiegele. Solving max-cut to optimality by intersecting semidefinite and polyhedral relaxations. *Mathematical Programming*, 121(2):307–335, 2008.

[RTV97] C. Roos, T. Terlaky, and J.-P. Vial. *Theory and algorithms for linear optimization: an interior point approach*. John Wiley & Son Ltd, 1997.

[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. *Physical Review Letters*, 119:040402, 2017.

[SBA+16] R. Schmied, J.-D. Bancal, B. Allard, M. Fadel, V. Scarani, P. Treutlein, and N. Sangouard. Bell correlations in a Bose-Einstein condensate. *Science*, 352(6284):441–444, 2016.

[SBWS18] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard. Certifying the building blocks of quantum computers from Bell's theorem. *Physical Review Letters*, 121:180505, 2018.

[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.

[Sch35] E. Schrödinger. Discussion of probability relations between separated systems. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 555–563. Cambridge University Press, 1935.

[Sch98] A. Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1998.

[SDCZ01] A. Sørensen, L.-M. Duan, J. Cirac, and P. Zoller. Many-particle entanglement with Bose–Einstein condensates. *Nature*, 409(6816):63, 2001.

[Sdpa] R. group of Masakazu Kojima. http://sdpa.sourceforge.net/index.html.

[SG01] V. Scarani and N. Gisin. Spectral decomposition of Bell's operators for qubits. *Journal of Physics A: Mathematical and General*, 34(30):6043, 2001.

[SG11] G. V. Steeg and A. Galstyan. A sequence of relaxations constraining hidden variable models. *arXiv:1106.1636*, 2011.

[ŠH16] I. Šupić and M. J. Hoban. Self-testing through EPR-steering. *New Journal of Physics*, 18(7):075006, 2016.

[SM01] A. S. Sørensen and K. Mølmer. Entanglement and extreme spin squeezing. *Physical Review Letters*, 86:4431–4434, 2001.

[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. *Physical Review Letters*, 115:250402, 2015.

[SU01] M. Seevinck and J. Uffink. Sufficient conditions for three-particle entanglement and their tests in recent experiments. *Physical Review A*, 65(1):012107, 2001.

[Sve87] G. Svetlichny. Distinguishing three-body from two-body nonseparability by a Bell-type inequality. *Physical Review D*, 35:3066–3069, 1987.

[SXL+17] C. Song, K. Xu, W. Liu, C.-p. Yang, S.-B. Zheng, H. Deng, Q. Xie, K. Huang, Q. Guo, L. Zhang, P. Zhang, D. Xu, D. Zheng, X. Zhu, H. Wang, Y.-A. Chen, C.-Y. Lu, S. Han, and J.-W. Pan. 10-qubit entanglement and parallel logic operations with a superconducting circuit. *Physical Review Letters*, 119:180511, 2017.

[TAS+14] J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, and A. Acín. Detecting nonlocality in many-body quantum states. *Science*, 344(6189):1256–1258, 2014.

[TAS+15] J. Tura, R. Augusiak, A. B. Sainz, B. Lücke, C. Klempt, M. Lewenstein, and A. Acín. Nonlocality in many-body quantum systems detected with two-body correlators. *Annals of Physics*, 362:370–423, 2015.

[Ter02] B. M. Terhal. Detecting quantum entanglement. *Theoretical Computer Science*, 287(1):313–335, 2002.

[TG05a] G. Tóth and O. Gühne. Detecting genuine multipartite entanglement with two local measurements. *Physical Review Letters*, 94:060501, 2005.

[TG05b] G. Tóth and O. Gühne. Entanglement detection in the stabilizer formalism. *Physical Review A*, 72:022340, 2005.

[TG06] G. Tóth and O. Gühne. Detection of multipartite entanglement with two-body correlations. *Applied Physics B*, 82(2):237–241, 2006.

[TGB06] G. Tóth, O. Gühne, and H. J. Briegel. Two-setting Bell inequalities for graph states. *Physical Review A*, 73:022303, 2006.

[TKGB09] G. Tóth, C. Knapp, O. Gühne, and H. J. Briegel. Spin squeezing and entanglement. *Physical Review A*, 79(4):042334, 2009.

[TKV+18] A. Tavakoli, J. Kaniewski, T. Vertesi, D. Rosset, and N. Brunner. Self-testing quantum states and measurements in the prepare-and-measure scenario. *arXiv preprint arXiv:1801.08520*, 2018.

[TSV+14] J. Tura, A. B. Sainz, T. Vértesi, A. Acín, M. Lewenstein, and R. Augusiak. Translationally invariant multipartite Bell inequalities involving only two-body correlators. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424024, 2014.

[VA15] L. Vandenberghe and M. S. Andersen. Chordal graphs and semidefinite optimization. *Foundations and Trends in Optimization*, 1(4):241–433, 2015.

[VAET14] G. Vitagliano, I. Apellaniz, I. L. Egusquiza, and G. Tóth. Spin squeezing and entanglement for an arbitrary spin. *Physical Review A*, 89(3):032307, 2014.

[VB96] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM review*, 38(1):49–95, 1996.

[WBIH94] D. J. Wineland, J. J. Bollinger, W. M. Itano, and D. J. Heinzen. Squeezed atomic states and projection noise in spectroscopy. *Physical Review A*, 50:67–88, 1994.

[WCL+16] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, and J.-W. Pan. Experimental ten-photon entanglement. *Physical Review Letters*, 117:210502, 2016.

[Wer89] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40:4277–4281, 1989.

[Wit15] P. Wittek. Algorithm 950: Ncpol2sdpa—sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables. *ACM Transactions on Mathematical Software*, 41(3):21:1–21:12, 2015.

[WKKM06] H. Waki, S. Kim, M. Kojima, and M. Muramatsu. Sums of squares and semidefinite program relaxations for polynomial optimization problems with structured sparsity. *SIAM Journal on optimization*, 17(1):218–242, 2006.

[WLB11] J. J. Wallman, Y.-C. Liang, and S. D. Bartlett. Generating nonclassical correlations without fully aligning measurements. *Physical Review A*, 83(2):022110, 2011.

[WLH+18a] X.-L. Wang, Y.-H. Luo, H.-L. Huang, M.-C. Chen, Z.-E. Su, C. Liu, C. Chen, W. Li, Y.-Q. Fang, X. Jiang, J. Zhang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan. 18-qubit entanglement with six photons' three degrees of freedom. *Physical Review Letters*, 120:260502, 2018.

[WLH+18b] X.-L. Wang, Y.-H. Luo, H.-L. Huang, M.-C. Chen, Z.-E. Su, C. Liu, C. Chen, W. Li, Y.-Q. Fang, X. Jiang, J. Zhang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan. 18-qubit entanglement with six photons' three degrees of freedom. *Physical Review Letters*, 120:260502, 2018.

[WSF+17] S. Wagner, R. Schmied, M. Fadel, P. Treutlein, N. Sangouard, and J.-D. Bancal. Bell correlations in a many-body system with finite statistics. *Physical Review Letters*, 119:170403, 2017.

[WW01] R. F. Werner and M. M. Wolf. All-multipartite Bell-correlation inequalities for two dichotomic observables per site. *Physical Review A*, 64:032112, 2001.

[Yal] J. Löfberg. https://yalmip.github.io.

[ZB02] M. Żukowski and Č. Brukner. Bell's theorem for general n-qubit states. *Physical Review Letters*, 88:210401, 2002.

[ZHW+15] C. Zhang, Y.-F. Huang, Z. Wang, B.-H. Liu, C.-F. Li, and G.-C. Guo. Experimental Greenberger–Horne–Zeilinger–type six-photon quantum nonlocality. *Physical Review Letters*, 115:260402, 2015.

[Zie12] G. M. Ziegler. *Lectures on polytopes*, volume 152. Springer Science and Business Media, 2012.

[ZKBL99] M. Zukowski, D. Kaszlikowski, A. Baturo, and J.-A. Larsson. Strengthening the Bell theorem: conditions to falsify local realism in an experiment. *arXiv preprint quant-ph/9910058*, 1999.

Acknowledgements

A first big thank you goes with no doubt to Antonio Acín, for giving me the opportunity to work in his group. Thank you for stimulating such a good mixture of easy-going, passionate and professional research environment among us. Then, I would also like to thank Fabio Sciarrino for the backstage role that he played in my PhD choice. Without his first advice, I would probably never have ended up moving to Barcelona.

Of course, a huge amount of thanks goes to all the members, past and present, of the QIT group: Dani, Paul, Ivan, Elsa, Markus, Bogna, Martí, Senaida, Karen, Gonzalo, Alejandro, Alexia, Mafalda, Flo, Ariel, Peter, Christian, Janek, Boris, Erik, Leo, Michał, Eric, Dario, Matteo, Joe, Osvaldo, Felix, Alex, Gabi, Korbinian, Chung-Yun, Patrick Jacopo, Moha, Zahra, Matteo (and to whomever I surely forgot, thank you as well). Between working days, coffee, darts and futbolín breaks, conferences and many dinners and nights out, each of you has contributed to make these four and a half years a very special time.

Among all the members, let me thank especially Dani, Jordi, Remik, Peter and Christian, for their inspiration and help through the projects we had together. I learnt a lot about science from all of you. I would also like to acknowledge all my other collaborators, namely Ivan, Alexia, Jed, Albert, Matteo, Jean-Daniel, Nicolas and Maciek. Thank you for the nice moments shared while working together.

How can I forget my YQIS fellows? Many thanks to Alexia, Boris and Alejandro for all the fun we had together, from attending the conference in Paris to organising all the details of our beautiful event in Barcelona. I am also very grateful to Alain and Sebastian, for being the initiators of this nice series of conferences and to Toni for giving the four of us this opportunity to organise its second edition.

During my PhD I have also had the great chance to visite other research groups. I would therefore want to thank Časlav for welcoming me in his group in Vienna. Those three months in such a friendly environment were a delightful parenthesis in my period in Barcelona. Special thanks go to Alessio, Giulia, Flaminia, Esteban and Costantino for con-

tributing to making me feel at home in Austria as well. And to Francesco for giving me the unique chance to voluntarily offer many goodbye drinks. Thanks a lot also to Nicolas Sangouard and all the nice members of his research group for welcoming me in Basel.

The first times of a PhD are especially though, but sharing the problems makes everything much easier to endure. For this, the Young PhD Students have been an enormous help. Alexia, Boris, Ivan and Leo, listing all the unique moments we shared would take a thesis by itself: thanks for being there during all this time.

Many thanks go also to the people oustide the QIT group that were part of this time in Barcelona, namely Marco, Sarah, Daniele, Bernat, Giulia, Livia, Francesco and Matteo. And also to all the old friends from Italy, especially the "sharks" Iolanda, Enrico, Cannizz, Stefano and Marco: I couldn't have imagined that so much fun can be shared even while being scattered around the world. I also want to apologise to Enrico, for not giving him a chance to contribute to the results of this thesis. I am sure his insight would have been invaluable.

Infine, vorrei ringraziare la mia famiglia per la fiducia e il supporto che mi ha dato in tutto questo periodo. E dulcis in fundo, a Simona, un grazie che racchiude una storia tutta sua.