
Certification of quantum states and measurements in contextuality scenarios



Author: Rafael Freitas dos Santos

Supervisor: dr hab. Remigiusz Augusiak

Centrum Fizyki Teoretycznej Polskiej Akademii Nauk

*A thesis submitted in partial fulfillment of the requirements
for the doctoral degree in physical sciences*

September 2023

*Dedicado aos meus avós (em especial D. Nizia,
e aos meus tios (em especial tia Cláudia).*

Abstract

Quantum theory is a probabilistic theory that provides a description of small-scale physical systems such as atoms or photons and it is one of the most successful physical theories that have been verified experimentally with a high degree of accuracy. At the same time it predicts phenomena such as quantum entanglement, Bell non-locality or more generally quantum contextuality that have been harnessed as resources for certain applications that are not accessible within classical physics. What is more, quantum phenomena are responsible for the recent rapid development of the new quantum technologies, just to mention the quantum computing machines. However, as far as the possibility of full exploitation of quantum technologies is concerned, this development has to be followed by designation of suitable certification tools that would enable the user to verify or certify that a given device operates according to its specification and generates the correct output. Such certification tools are particularly relevant in the context of quantum cryptography where the communicating parties need to verify that the state shared by the parties as well as the measurements performed by them are the correct one.

While there exist methods that serve the above purpose such as for instance the well-known quantum tomography, these rely on certain assumptions such as that the measuring devices used to test the state are fully characterized and that the user can trust that they perform correct measurements. While in certain situations such assumptions are justified, they are not when it comes to such tasks as quantum cryptography. As a remedy to this problem the idea of self-testing was put forward by Mayers and Yao. It allows for almost complete characterization of the underlying quantum systems based on the nonclassical correlations they produce, without the need of making strong assumptions about them. It thus falls into the category of device-independent certification in which quantum devices are treated as black boxes whose internal working is unknown to the user and the nonclassicality they generate is used to make nontrivial statements about them.

Self-testing as originally put forward by Mayers and Yao is based on Bell nonlocality and allows for certification of entangled states and the measurement performed on them. While many self-testing methods have already been proposed for entangled quantum states both in the bipartite and multipartite case, most of them, in particular, in the multipartite case, are devoted to systems that are locally qubits. Moreover, this type of certification methods have barely been explored for systems that do not have spatially separated subsystems and thus do not give rise to Bell nonlocality. Our aim here is to fill the above gaps. On one hand, we explore the possibility of exploiting quantum contextuality for certification purposes. In this direction we provide a class of scalable noncontextuality inequalities whose maximal violations can be used for certification of quantum systems consisting of N qubits and sets of binary measurements that obey certain commutation and anticommutation relations and generate the N -qubit Pauli group. Second, we propose a scheme, which is a modification of the standard quantum contextuality scenario, which allows for making certification statements about quantum systems from the observed correlations, however, without making any assumptions about the compatibility structure of the involved measurements which are made in contextuality-based approaches. On the other hand, we introduce the first, to the best of our knowledge, general class of Bell inequalities that are maximally violated by the multipartite graph states of arbitrary prime local dimension and show that in the qutrit case the maximal quantum violation of these inequalities allows for self-testing of the graph states. Again, our inequalities are scalable in the sense that the number

of expectation values they consist of scales linearly with the number of parties which is relevant from the point of view of their experimental exploitation.

Streszczenie

Teoria kwantowa to teoria probabilistyczna, która opisuje układy fizyczne o małej skali, takie jak atomy czy fotony, i jest jedną z najskuteczniejszych teorii fizycznych, które zostały zweryfikowane eksperymentalnie z dużą dokładnością. Jednocześnie przewiduje zjawiska takie jak splątanie kwantowe, nielokalność Bella czy bardziej ogólnie kontekstualność kwantową, które zostały przekute w zasoby dla pewnych zastosowań, które nie są dostępne w fizyce klasycznej. Co więcej, zjawiska te są odpowiedzialne za szybki rozwój nowych technologii kwantowych, który się w ostatnim czasie odbywa, żeby tylko wspomnieć komputery kwantowe. Z punktu widzenia możliwości pełnego wykorzystania technologii kwantowych, za tym rozwojem musi podążać tworzenie odpowiednich narzędzi certyfikujących, które umożliwiłyby klasycznemu użytkownikowi sprawdzenie lub poświadczenie, że dane urządzenie działa zgodnie ze swoją specyfikacją i generuje prawidłowy wynik. Takie narzędzia certyfikacji są szczególnie istotne w kontekście kryptografii kwantowej, gdzie komunikujące się strony muszą zweryfikować, czy stan udostępniany przez strony, jak również wykonane przez nie pomiary są prawidłowe.

Pomimo tego, że istnieją metody służące powyższemu celowi, jak na przykład dobrze znana tomografia kwantowa, opierają się one na pewnych założeniach, takich jak to, że urządzenia pomiarowe używane do badania stanu są w pełni scharakteryzowane i że użytkownik ma pewność, że wykonują prawidłowe pomiary. O ile w niektórych sytuacjach takie założenia są uzasadnione, o tyle przypadku takich zadań jak kryptografia kwantowa już nie. Jako remedium na ten problem, Mayers i Yao zaproponowali ideę samotestowania. Pozwala ono na niemal pełną charakteryzację układów kwantowych w oparciu o wytwarzane przez nie korelacje nieklasyczne, bez konieczności czynienia założeń na temat tych urządzeń. Samotestowanie jest zatem sposobem certyfikacji w wersji niezależnej od urządzeń (ang. *device-independent*), w której urządzenia kwantowe są traktowane jak czarne skrzynki, których wewnętrzne działanie jest nieznane dla użytkownika, a nieklasyczność, jaką generują, jest tym zasobem, który pozwala wyciągać nietrywialne wnioski na ich temat.

Samotestowanie, w swoim pierwotnym sformułowaniu opiera się na nielokalności Bella i umożliwia certyfikację stanów splątanych i wykonanych na nich pomiarów kwantowych. Choć powstało już wiele metod samotestowania splątanych stanów kwantowych zarówno w przypadku dwuciałowym, jak i wieloczęściowym, większość z nich, szczególnie w tym drugim przypadku, poświęcona jest układom składającym się z kubitów. Co więcej, metody certyfikacji tego typu są rzadko badane w przypadku układów, które nie mają podukładów oddzielonych przestrzennie i tym samym nie wykazują nielokalności Bella. Naszym celem jest wypełnienie powyższych luk. Z jednej strony badamy możliwość wykorzystania kontekstowości kwantowej do celów certyfikacji. W tym kierunku wprowadzamy klasę skalowalnych nierówności niekontekstualnych, których maksymalne łamanie kwantowe można wykorzystać do certyfikacji układów kwantowych składających się z N kubitów i zbiorów pomiarów binarnych, które spełniają pewne relacje komutacyjne i antykomutacyjne i generują N -kubitową grupę Pauliego. Po drugie, proponujemy schemat, który jest modyfikacją standardowego scenariusza kontekstualności kwantowej, a który pozwala na formułowanie certyfikujących o układach kwantowych na podstawie zaobserwowanych korelacji, ale bez konieczności czynienia założeń na temat struktury kompatybilności wykonywanych pomiarów, które się standardowo czyni w przypadku metod certyfikacji opartych na standardowej kontekstualności. Z drugiej strony rozwijamy zastosowanie nielokalności Bella, która jest pewną szczególną formą kwantowej kontekstualności, w samotestowaniu. Wprowadzamy pierwszą,

zgodnie z naszą najlepszą wiedzą, ogólną klasę nierówności Bella, które są maksymalnie łamane przez wielocząstkowe stany grafowe o dowolnym wymiarze lokalnym, który liczbą pierwszą, a także pokazujemy, że w przypadku kutrytowym maksymalne łamanie tych nierówności pozwala na samotestowanie stanów grafowych. Podobnie jak w powyższym przypadku nasze nierówności są skalowalne w tym sensie, że liczba wartości oczekiwanych, z których się składają skaluje się liniowo z liczbą podukładów co ma znaczenie z punktu widzenia ich zastosowań w eksperymencie.

Declaration

The work described in this thesis was undertaken between December 2018 and June 2023 while the author was a research student under the supervision of dr. hab. Remigiusz Augusiak at the Center for Theoretical Physics of the Polish Academy of Sciences. No part of this thesis has been submitted for any other degree at the same institute or any other scientific institution.

This doctoral thesis is in the form of a collection of the following three scientific publications:

- D. Saha, R. Santos, R. Augusiak, *Sum-of-squares decompositions for a family of noncontextuality inequalities and self-testing of quantum devices*, *Quantum* **4**, 302 (2020).
- R. Santos, J. Chellasamy, R. Augusiak, *Scalable noncontextuality inequalities and certification of multiqubit quantum systems*, *Physical Review A* **106**, 012431 (2022).
- R. Santos, D. Saha, F. Baccari, R. Augusiak, *Scalable Bell inequalities for graph states of arbitrary prime local dimension and self-testing*, *New Journal of Physics* **25**, 063018 (2023).

The thesis is composed of five chapters. Chapter 1 is an introduction to the thesis. The next three chapters, Chapter 2, 3 and 4 contain the research papers listed above, one for each chapter. Each of these chapters is also supplemented with a brief summary of the obtained results and with my statement of authorship. The Chapter 5 contains the conclusions and final remarks of the thesis.

Acknowledgements

I would like to thank the Foundation for Polish Science for their support through the First Team project (No First TEAM/2017-4/31) co-financed by the European Union under the European Regional Development Fund.

Contents

1	Introduction	1
1.1	Probabilistic theories and a notion of classicality	3
1.1.1	A notion of classicality based on a noncontextual hidden variable model	5
1.2	Quantum theory	7
1.3	Quantum theory as a contextual theory	10
1.3.1	State-dependent quantum contextuality	11
1.3.2	State-independent quantum contextuality	13
1.4	Quantum theory as a nonlocal theory	14
1.5	Entanglement	18
1.5.1	Graph states	20
1.6	Self-testing	23
2	Paper I	27
2.1	Sum-of-squares decompositions for a family of noncontextuality inequalities and self-testing of quantum devices	27
2.2	Author's contribution	28
3	Paper II	41
3.1	Scalable noncontextuality inequalities and certification of multiqubit quantum systems	41
3.2	Author's contribution	42
4	Paper III	60
4.1	Scalable Bell inequalities for graph states of arbitrary prime local dimension and self-testing	60
4.2	Author's contribution	61
5	Concluding remarks	92

Chapter 1

Introduction

Quantum theory is a probabilistic theory that allows to describe physical phenomena of small-scale systems such as atoms or photons and it is one of the most successful physical theories that have been verified experimentally with a high degree of accuracy. Indeed, it enabled correct explanations of such phenomena as black-body radiation, provided by Planck, or the photoelectric effect, provided by Einstein, which at that time could not be described within existing theories. The development of quantum theory was certainly a breakthrough in the history of science that came out with an intriguing description that raises deep philosophical questions about nature and today it is the foundation for emerging and promising technologies such as quantum computers.

On the other hand, quantum theory required a drastic change in the way we perceive and describe physical phenomena. In particular, the probabilistic nature of quantum theory led Einstein, Podolsky and Rosen [1] in their famous article published in 1935 to consider a thought experiment involving entangled states with which they argued quantum theory is incomplete. Then, they speculated whether quantum theory can be made complete by adding some extra (hidden) variables that were not a part of the theory, but would remove unpredictability from it. The idea of hidden variables was a subject of debate among physicists until 1964 when Bell proved that they are not enough to explain all predictions of quantum theory [2]. To this aim, he devised another thought experiment involving entanglement which gave rise to correlations violating a certain inequality which is satisfied by any theory built on the concept of hidden variables. The existence of correlations violating Bell inequalities is nowadays referred to as Bell nonlocality.

Many experiments have been designed since then to confirm the existence of Bell nonlocality and, at the same time, to prove the incompatibility between predictions of quantum theory and the local hidden variable models, just to mention the experiments performed by Freedman and Clauser in 1972 [3], or by Aspect, Dalibard and Roger [4] in 1988, or, the more recent one carried out by Hensen *et al.* [5] in which it was possible to close all the relevant loopholes. Importantly, the early attempts to experimentally confirm violations of Bell inequalities by quantum theory were acknowledged by awarding A. Aspect, J. F. Clauser and A. Zeilinger the Nobel prize in physics in 2022. (For a broad review about Bell nonlocality we recommend [6].)

Later it turned out possible to extend the framework of local hidden variable models to more general scenarios where entanglement or space-like separation used in composite systems is not needed to show the discrepancy between the predictions of quantum theory and the hidden variable models. This leads to the notion of noncontextuality described for the first time by Kochen and Specker [7].

Nonlocality, in the sense of Bell, can be interpreted as a special case of contextuality. Many efforts have been devoted in the last decades to exploring, characterizing, and understanding the phenomena of Bell nonlocality and contextuality in the context of quantum theory, and also to propose quantifiable schemes that can be experimentally used to confirm the “weirdness” of quantum theory (cf. Refs. [3], [4], [8]). Most of these efforts are based on violations of Bell or, more generally, noncontextuality inequalities by quantum theory. The most famous such inequalities are the Clauser-Horne-Shimony-Holt (CHSH) inequality [9] in the context of Bell nonlocality and Klyachko-Can-Binicioğlu-Shumovsky (KCBS) inequality [10] in the contextuality case.

The unintuitive properties of quantum theory, like entanglement and related to it Bell nonlocality or, more generally, quantum contextuality, which can be seen as various forms of nonclassicality that show the discrepancy between the classical and quantum theories, are also resources for information processing. In this context, the works on communication complexity [11], information theory [12], [13] and quantum cryptography [14], [15] should be mentioned. More recently it was pointed out that Bell nonlocality can also be used for certification purposes. Let us stress that the need for designing certification schemes for quantum states follows from the recent rapid development of new quantum technologies such as quantum cryptography systems or quantum computing devices. In fact, the possibilities that these technologies offer can only be fulfilled if the classical user is able to certify that the new devices work according to their specification and generate the correct output. It is also worth pointing out that the need for efficient certification methods was also highlighted in the Quantum Manifesto [16].

The first ones to propose the exploitation of nonclassical correlations as a resource for certification were Mayers and Yao, who put forward the concept of *self-testing* [17] (see also the recent review [18]). It allows one to device-independently certify entangled quantum states and measurements performed on them from the observed nonlocal correlations. The term “device-independent”, tossed for the first time in the context of quantum cryptography in Ref. [14], refers to the fact that to verify or certify a quantum state or measurements performed on it, no assumptions on that quantum objects are made, and one uses only the statistical data generated by that system. Since then many self-testing results have been derived for various quantum states and measurements (see, e.g., Refs. [19]–[24]). Also, the concept of self-testing was generalized to the case of quantum contextuality to enable certification of quantum systems that do not exhibit entanglement [25].

The main goal of this thesis is to develop certification schemes for quantum systems based on the above forms of nonclassicality. More specifically, on one hand, we further explore the possibility of exploiting quantum contextuality for certification purposes. In this direction, we provide a class of scalable noncontextuality inequalities whose maximal violations can be used for certification of quantum systems consisting of N qubits and sets of binary measurements that obey certain commutation and anticommutation relations and generate the N -qubit Pauli group. Second, we propose a scheme, which is a modification of the standard quantum contextuality scenario, which allows for making certification statements about quantum systems from the observed correlations, however, without making any assumptions about the compatibility structure of the involved measurements which are made in contextuality-based approaches. On the other hand, we introduce the first, to the best of our knowledge, a general class of Bell inequalities that are maximally violated by the multipartite graph states of arbitrary prime local dimension and show that in the qutrit case the maximal quantum violation of these inequalities allows for self-testing of the graph states. Again, our inequalities are scalable in the

sense that the number of expectation values they consist of scales linearly with the number of parties which is relevant from the point of view of their experimental exploitation.

In the remainder of this chapter we discuss the main ideas and mathematical formalism that we use in later parts of the thesis. In Sec. 1.1 we introduce a general framework for probabilistic theories and a notion of classicality based on hidden-variable models. Then, in Sec. 1.2, we describe the basic axioms of quantum theory, whereas in Secs. 1.3 and 1.4 we show examples of quantum systems that exhibit quantum contextuality and nonlocality, respectively. The notion of quantum entanglement is presented in Sec. 1.5 as a basic concept in quantum theory. Finally, in Sec. 1.6, we discuss the mathematical formalism of self-testing, crucial for the certification schemes proposed in this thesis.

1.1 Probabilistic theories and a notion of classicality

In this section, we outline the general notions and suitable mathematical framework used in the description of experiments performed on the considered physical systems. Throughout this thesis, we adopt an operational view of preparations and measurements, sufficiently general to encompass classical probability theory, quantum theory, and even generalized probabilistic theories. Similar approaches are discussed more in-depth in Refs. [26], [27].

The suitable assumptions we need here are about the nature of the experiments that can be performed on a physical system. These assumptions pertain to the two types of available actions: preparations - such as the generation of a quantum state - and operations - such as measurements. An important assumption is that these experiments are reproducible, they can be performed as many times as needed and we can use multiple repetitions of a given procedure to count relative frequencies. For each operation performed over a preparation, there may be a finite set of outcomes, each occurring with a well-defined probability depending on the underlying physical system. Also, there exist operations that are performed in a sequence provided they do not demolish the physical system. Preparations can be compared through the observed statistics in relation to the operations performed on them, and the equivalence class of these statistics defines a physical state.

Before going into a more specific theory, i.e. the quantum theory, we formulate a few very general definitions establishing a framework that will be our playground for the rest of the thesis.

Definition 1 (States). *Two preparations are equivalent if they give rise to the same probability distributions in relation to all operations. The equivalence class of preparations is called a state.*

This notion of states defines, from an operational point of view, what can be inferred about a physical system. In other words, it expresses the maximal amount of information that can be accessed via performing available operations on it. If two physical objects exhibit the same behavior for all the available operations they cannot be distinguished and therefore they belong to the same class, which we name by state.

Definition 2 (Measurements). *Measurements are operations with more than one outcome.*

Every measurement performed on a physical system reveals a possible outcome. For instance, in the Stern-Gerlach experiment, the effect of a non-homogeneous magnetic field splitting the beam of atoms into two other beams up and down can be modeled as a measurement with two outcomes. Another example is a measurement of the temperature in a city at a certain time; it is a process of

revealing a number that has a physical meaning. In this case, the measurement has a continuous range of outcomes. In this thesis, we focus on measurements with a finite number of outcomes. Let us now move on to the notion of compatibility of measurements.

Definition 3 (Compatibility). *Given a set of measurements $\{A_1, A_2, \dots, A_n\}$, we say that they are compatible if they can be performed jointly or sequentially without changing the statistics of outcomes.*

The concept of compatibility of measurements in a physical system is the key point to address. Based on our classical intuition, we tend to think that measurements are always compatible, i.e., they can be performed without disturbing each other like the measurements of the position and the speed of a car.

In this general framework of probabilistic theories, the meaning of compatibility is associated with the resulting statistics after many runs of an experiment done to collect the frequencies of the outcomes. We say that measurements are compatible if the outcome statistics obtained after many runs of an experiment are not disturbed by each other.

Definition 4 (Context). *A context is a set of compatible measurements.*

Having all the necessary notions at hand, we can now define the contextuality scenario within the framework of generalized probabilistic theories to be a triple of sets: a set of measurements that can be performed on a physical system, a set of outcomes of these measurements and a set of contexts.

In order to set up a notation, let $\{A_1, \dots, A_n\}$ be a set of measurements that can be performed on a system, all of them having a finite number of outcomes, and let C_i be subsets of that set, $C_i \subset \{A_1, \dots, A_n\}$, that define contexts. Now, for a given context $C = \{A_{i_1}, \dots, A_{i_k}\}$ with $i_1 < i_2 < \dots < i_k = 1, \dots, m$ with $m \leq n$, we can perform measurements and with the respective frequencies, approximate the corresponding probability distribution. After many runs of the experiment, one may obtain satisfactory approximation for probability distributions $p(\vec{a}_C | \vec{A}_C)$ of obtaining outcomes $a_{i_1}, \dots, a_{i_k} := \vec{a}_C$ after performing the measurements $A_{i_1}, \dots, A_{i_k} := \vec{A}_C$. With this probability distribution, for each context C we can calculate the expectation value defined as:

$$\langle A_{i_1} \dots A_{i_k} \rangle_C = \sum_{a_i} a_{i_1} \dots a_{i_k} p(a_{i_1}, \dots, a_{i_k} | A_{i_1}, \dots, A_{i_k}). \quad (1.1)$$

The contextuality experiment is then described by a collection of probability distributions $\{p(\vec{a}_{C_i} | \vec{A}_{C_i})\}$ corresponding to all contexts C_i . In what follows we denote this collection by

$$\vec{p} = \bigcup_i \{p(\vec{a}_{C_i} | \vec{A}_{C_i})\} \quad (1.2)$$

and call it simply correlations or behavior.

Let us now illustrate the above definition with two paradigmatic scenarios often considered in the literature, which are the Clauser-Horne-Shimony-Holt (CHSH) scenario [9] and the Klyachko-Can-Binicioğlu-Shumowski (KCBS) scenario [10]. Fig. 1.1 presents the compatibility graphs corresponding to each of the scenarios in which vertices represent measurements whereas edges represent compatibility relations between measurements, in the sense that two measurements are compatible if and only if they are connected by an edge.

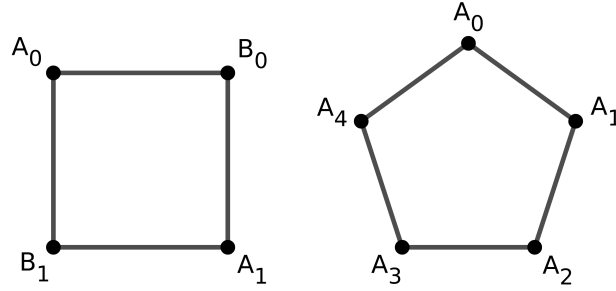


Figure 1.1: Compatibility graphs of the CHSH (left) and KCBS (right) scenarios. The vertices represent the measurements, whereas the edges indicate compatibility relations between them: two measurements are compatible if they are connected by an edge. In both scenarios, all the measurements have two outcomes.

The CHSH scenario comprises four measurements that we denote by A_0, A_1, B_0, B_1 . Each of them have two outcomes, labeled by ± 1 . The contexts in this scenario are the four pairs of measurements $\{A_i, B_j\}$ with $i, j \in \{0, 1\}$. The KCBS scenario consists of a set of five measurements that we denote by A_0, A_1, A_2, A_3, A_4 ; all of them have two outcomes, which we also label as ± 1 . In this scenario the contexts are the pairs of measurements $\{A_i, A_{i+1}\}$ with $i = 0, \dots, 4$ where this sum is modulo 5.

In the CHSH scenario there are 16 probabilities, denoted by $p(a, b|A_i, B_j)$, that describe the experiment, so the probability space belongs to \mathbb{R}^{16} . For any pair $i, j = 0, 1$, these joint probabilities respect the normalization condition: $\sum_{a,b} p(a, b|A_i, B_j) = 1$.

Analogously, in the KCBS scenario the probability space is a bounded subset of \mathbb{R}^{20} since there are 20 probabilities forming the behavior, i.e., $p(a_i, a_{i+1}|A_i, A_{i+1})$. These satisfy $\sum_{a_i, a_{i+1}} p(a_i, a_{i+1}|A_i, A_{i+1}) = 1$ for every $i = 0, \dots, 4$.

1.1.1 A notion of classicality based on a noncontextual hidden variable model

To start the discussion about classicality, let us suppose that we want to model an ideal gas consisting of a number of particles of the order of 10^{23} . A possible way to do this is to directly employ the Newton's laws, but this would require solving 10^{23} differential equations of the second order to calculate the position and velocity of all these particles which is an unfeasible task for the existing computing devices. Instead, we can focus on statistical properties only, which are often sufficient to solve practical problems. In this case, the statistical description is due to a lack of knowledge of the behavior of all these 10^{23} particles.

The question of how probabilities emerge in the mathematical descriptions of physical systems is a key point here. In classical statistical physics, for instance, probabilities arise as a description of a physical system due to the lack of complete knowledge of it. However, it is assumed, that there exist some extra variables (positions and velocities of all particles), that are discarded when measuring the pressure or the temperature. As we will see here, quantum theory is something more in the sense that there might not exist any physical “real” variables underlying the observed probability distributions.

With this motivation, we introduce the mathematical definition of a non-contextual hidden variable model:

Definition 5 (Non-contextual hidden variable model). *Given a contextuality scenario, we say that the distributions of probabilities admit a non-contextual hidden variable model if for every context $C = \{A_{i_1}, \dots, A_{i_k}\}$, the corresponding joint probabilities can be written as*

$$p(\vec{a}_C | \vec{A}_C) = \sum_{\lambda} p(\lambda) p(a_{i_1} | A_{i_1}, \lambda) \dots p(a_{i_k} | A_{i_k}, \lambda), \quad (1.3)$$

where λ belongs to a set of extra-variables, traditionally referred to as hidden variables and $p(a_i | A_i, \lambda)$ are probability distributions corresponding to single measurements.

Thanks to the Abramsky-Brandenburg (AB) theorem [28], to characterize the correlations that admit non-contextual hidden variable models is enough to take the convex-hull of all models for which all probability distributions $p(a_i | A_i, \lambda)$ are deterministic; in fact, the set of correlations admitting the NCHV models is a polytope. The AB theorem is a generalization of the famous Fine theorem [29] which was proved in the context of Bell nonlocality. Consequently, to evaluate the maximum of a linear expression in the elements of \vec{p} it is enough to restrict the optimization to only the finite set of deterministic strategies. We will illustrate this concept with two examples of linear expressions, one defined within the CHSH scenario and one within the KCBS scenario.

The first example of a linear expression, related to the CHSH scenario, reads

$$I_{CHSH} := \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq \eta_C = 2, \quad (1.4)$$

and gives rise to the famous CHSH Bell inequality [9]. By η_C we denoted the maximal value of I_{CHSH} over the NCHV models (1.3). In order to determine the latter it is enough to observe that for the deterministic NCHV models, for which $\langle A_i B_j \rangle = \langle A_i \rangle \langle B_j \rangle$ and $\langle A_i \rangle, \langle B_j \rangle = \pm 1$ for all i, j , the value of I_{CHSH} , which is a linear expression, can be only ± 2 . To see that explicitly, let us observe that for the algebraic expression $a_0(b_0 + b_1) + a_1(b_0 - b_1)$, where $a_i, b_j \in \{\pm 1\}$, we have two possibilities to take into account, $b_0 = b_1$ or $b_0 \neq b_1$. In both cases the remaining expression will be $\pm 2a_i$, and therefore the maximal value of I_{CHSH} is 2.

In the case of KCBS scenario [10] we consider the expression

$$I_{KCBS} := \langle A_0 A_1 \rangle + \langle A_1 A_2 \rangle + \langle A_2 A_3 \rangle + \langle A_3 A_4 \rangle - \langle A_4 A_0 \rangle \leq \eta_C = 3. \quad (1.5)$$

To show that the maximal value of I_{KCBS} over the NCHV models is $\eta_C = 3$, we can again restrict our attention to the deterministic strategies. One would naively expect this maximal value to be 5, however, this is impossible since the term $-\langle A_4 A_0 \rangle$ would have to be equal to -1 and the other terms to be 1. This is of course impossible to achieve by simply replacing averages $\langle A_i A_{i+1} \rangle$ with $a_i a_{i+1}$, where $a_i \in \{-1, 1\}$. If we try to attain 4 we face the same problem. However, 3 can be attained if we choose all the measurements to have the same outcome.

Another important concept to introduce here is the non-disturbance condition. If a subset of measurements belongs to two different contexts, the marginals for this subset of measurements obtained from the probability distributions corresponding to these contexts must coincide. To clarify the non-disturbance condition let us take an example. In the CHSH scenario the measurement A_0 belongs to

two different contexts. Suppose then that we want to calculate the probability of the outcome 1. For this measurement we can choose two contexts, one with the measurement B_0 or the other with B_1 . Then, the following condition must be satisfied:

$$p(1|A_0) = \sum_b p(1, b|A_0, B_0) = \sum_b p(1, b|A_0, B_1). \quad (1.6)$$

In the case of composite systems, the non-disturbance condition corresponds to the non-signaling condition, which we will discuss later in Sec. 1.4.

As in Eq. (1.6), the non-disturbance condition can be expressed by a finite set of linear equations for the elements of \vec{p} , and so correlations satisfying this condition also form a polytope, obtained by intersecting the polytope of arbitrary probability distributions by a finite set of the hyperplanes representing the above linear constraints. Every behavior \vec{p} that admits the NCHV model satisfies the non-disturbance condition. Thus, the classical set of probabilities is a polytope that belongs to the non-disturbance polytope.

We say that a probabilistic theory is contextual if this theory gives rise to correlations \vec{p} that cannot be described by a non-contextual hidden variable model. A way to show that a probabilistic theory is contextual is to provide an example of a \vec{p} that violates some noncontextuality inequality such as for instance the CHSH or the KCBS ones discussed above. As we will see in Sec. 1.3, quantum theory is an example of a contextual theory.

1.2 Quantum theory

A very special example of a probabilistic theory is quantum theory. In this section, we present the rules that define this theory and that are important in this thesis. These rules describe how the probabilities are calculated when modelling a quantum system composed of a state and measurements. In order to do this we first need to introduce some basic mathematical concepts. The mathematical background of quantum theory is functional analysis and the first definition we introduce here is that of a Hilbert space:

Definition 6 (complex Hilbert space). *A Hilbert space is a complex vector space \mathcal{H} which is equipped with an inner product and is complete in the norm induced by this inner product.*

The Reader is referred to as Ref. [30] for a more in-depth discussion about Hilbert spaces. In this thesis, we focus on measurements that have a finite number of outcomes and Hilbert spaces with finite dimensions are enough to describe the quantum systems. A simple example of a finite-dimensional Hilbert space is \mathbb{C}^d which consists of d -dimensional complex vectors and is equipped with the canonical inner product. As any Hilbert space of dimension d is actually isomorphic to \mathbb{C}^d , in this thesis we simply assume that our playground is $\mathcal{H} \cong \mathbb{C}^d$.

Having introduced the notion of Hilbert spaces, we can now define the mathematical objects representing quantum states and measurements. Quantum states are represented by density operators acting on the corresponding Hilbert space and quantum measurements are represented by sets of positive semi-definite operators or, equivalently, Hermitian operators in the case of projective measurements. Let us now define the above notions in a more formal way.

Definition 7 (Density Operator). *A density operator $\rho : \mathcal{H} \rightarrow \mathcal{H}$ is a positive semi-definite operator with $\text{Tr}(\rho) = 1$. A density operator represents a state of a quantum system.*

The set of density operators is convex since any convex combination of two density operators is positive semi-definite too and has trace one, therefore it is a density operator.

Definition 8 (Pure states). *Pure states are extremal elements of the set of the density operators.*

The extremal elements are those that cannot be written as a convex combination of two other different density operators, so they are rank-one projectors. In other words, pure states correspond to density matrices that can be written as $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle$ is an normalized vector from the corresponding Hilbert space \mathcal{H} . Thus, up to a phase factor, pure states are represented by normalized elements $|\psi\rangle$ from the Hilbert space \mathcal{H} .

The simplest non-trivial quantum systems of interest are qubits. These are represented by density operators acting on a two-dimensional Hilbert space $\mathcal{H} \cong \mathbb{C}^2$ which can be expressed as:

$$\rho = \frac{1}{2}(\mathbb{I} + a_x X + a_y Y + a_z Z), \quad (1.7)$$

where the vector $\vec{a} = (a_x, a_y, a_z) \in \mathbb{R}^3$ and $\|\vec{a}\| \leq 1$, \mathbb{I} is the identity operator on \mathcal{H} , and X, Y and Z are the Pauli matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (1.8)$$

Thus, every density operator on \mathbb{C}^2 can be represented by a three-dimensional real vector \vec{a} with norm $\|\vec{a}\| \leq 1$. Within this representation, the case of $\|\vec{a}\| = 1$ corresponds to pure states, and, that of $\|\vec{a}\| < 1$ to mixed states; in particular, for $\vec{a} = 0$ one obtains the maximally mixed state $\rho = \frac{1}{2}\mathbb{I}$.

Let us denote by $|0\rangle$ and $|1\rangle$ the normalized eigenvectors of the Pauli matrix Z corresponding to the eigenvalues 1 and -1 , respectively. These vectors define an orthonormal basis for the Hilbert space $\mathcal{H} = \mathbb{C}^2$, meaning that any normalized element of this Hilbert space can be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1.9)$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. Analogously, we denote by $|+\rangle$ and $|-\rangle$ the normalized eigenvectors, with respective eigenvalues 1 and -1 , of the Pauli matrix X , and observe that they form another orthonormal basis in $\mathcal{H} \cong \mathbb{C}^2$.

For further purposes let us notice that for qudit systems, the Pauli matrices X and Z can be generalized as follows:

$$Z = \sum_{k=0}^{d-1} \omega^k |k\rangle\langle k|, \quad X = \sum_{k=0}^{d-1} |k+1\rangle\langle k|, \quad (1.10)$$

where the index k is modulo d and $\omega = \exp(2\pi i/d)$ is the d -th root of unity.

Let us now move to the mathematical description of a quantum measurement and introduce the definition of positive operator valued measure (POVM) which is the most general description of it.

Definition 9 (POMV). *A measurement in quantum theory is represented by positive operators valued measure (POVM). A measurement A with d outcomes labeled by the set $\{0, 1, \dots, d-1\}$ is represented*

by a set of respective d positive semi-definite operators P_0, P_1, \dots, P_{d-1} acting on \mathcal{H} such that

$$P_0 + \dots + P_{d-1} = \mathbb{I}, \quad (1.11)$$

where \mathbb{I} is the identity operator acting on \mathcal{H} .

Definition 10 (Projective measurements). *Projective measurements are measurements where the positive operators P_1, \dots, P_d are pairwise orthogonal projectors, that is, $P_i P_j = \delta_{ij} P_i$ ($i, j = 0, 1, \dots, d-1$).*

Let us illustrate the above notion with a simple example of a two-outcome projective measurement given by a two-element set $\{P_0, P_1\}$, where $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$; the outcomes of this measurement are labelled $a_0 = 1$ and $a_1 = -1$. First, one observes that these projectors satisfy the condition (1.11), that is,

$$P_0 + P_1 = |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{I} \quad (1.12)$$

and that they are orthogonal. Another representation of a projective measurement, equivalent to the above one, is in terms of a quantum observable. Precisely, to a set of mutually orthogonal projections $\{P_i\}$ one can associate a Hermitian operator $A = \sum_i a_i P_i$ whose eigenvalues are the outcomes of the respective measurement. One calls such a Hermitian operator quantum observable; its spectral decomposition contains all the information about the projectors. For instance, for the above exemplary two-outcome measurement can be represented by the following observable

$$A = +1|0\rangle\langle 0| - 1|1\rangle\langle 1|, \quad (1.13)$$

which is basically the Z Pauli matrix. As we will see later, the representation of projective quantum measurements in terms of observables turns out to be very useful to when computing expectation values.

The maximal information that can be obtained about a quantum system are probabilities of obtaining outcomes of measurements performed on it. Given the mathematical descriptions of quantum states and measurements, we now are able to describe how probabilities are expressed in quantum theory. This is done via the Born's rule defined as:

Definition 11 (Born's rule). *The probability of the outcome a_i when the projective measurement A is performed in the state ρ is given by*

$$p(a_i|A) = \text{Tr}(\rho P_i). \quad (1.14)$$

Moreover, the post-measurement state corresponding to the outcome a_i is given by

$$\frac{P_i \rho P_i}{\text{Tr}(P_i \rho P_i)}. \quad (1.15)$$

Suppose now we perform the projective measurement represented by the observable A in Eq. (1.13) on a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The probabilities of obtaining the outcomes 1 and -1 are given by:

$$p(1|A) = \text{Tr}(|\psi\rangle\langle\psi||0\rangle\langle 0|) = |\langle\psi|0\rangle|^2 = |\alpha|^2, \quad (1.16)$$

$$p(-1|A) = \text{Tr}(|\psi\rangle\langle\psi||1\rangle\langle 1|) = |\langle\psi|1\rangle|^2 = |\beta|^2. \quad (1.17)$$

Notice that the normalization condition is satisfied because $p(1|A) + p(-1|A) = |\alpha|^2 + |\beta|^2 = 1$. In this

case the orthonormal basis used to express the state $|\psi\rangle$ is exactly the eigenbasis of the observable and this is why the probabilities are exactly $|\alpha|^2$ and $|\beta|^2$. The expectation value of A on the state $|\psi\rangle$ is given by

$$\langle A \rangle_\psi = +1p(1|A, \psi) - 1p(-1|A, \psi) = \text{Tr}(|\psi\rangle\langle\psi|A) = \langle\psi|A|\psi\rangle. \quad (1.18)$$

This simple example demonstrates the utility of the notion of quantum observables in computing the mean values.

Now, let us notice that if the same measurement is performed twice in a sequence, the probability of obtaining the same outcome is one, so the measurements in quantum theory respect a condition of repeatability. For instance, suppose that after the measurement A was performed on $|\psi\rangle$, we obtained the outcome $+1$. According to Eq. (1.15) the state after the measurement is given by

$$\frac{|0\rangle\langle 0|\psi\rangle\langle\psi|0\rangle\langle 0|}{|\alpha|^2} = |0\rangle\langle 0|. \quad (1.19)$$

Now, if the measurement A is performed again on the above state, the experimenter will observe the same outcome with probability 1. The same happens if the first measurement yields the outcome -1 . At this point we are ready to introduce the notion of compatibility of measurements in quantum theory.

Definition 12 (Compatible quantum measurements). *We then say that a pair of projective measurements represented by the observables A_i and A_j are compatible if, and only if, $[A_i, A_j] = 0$.*

The above definition extends directly to the case of more measurements: a set of measurements A_1, \dots, A_n is compatible iff any pair of measurements from that set commute. Now, given a set of pairwise compatible projective quantum measurements A_1, \dots, A_n , we can calculate the expectation value for this set of measurements (which can be performed jointly or in sequence) by:

$$\langle A_1 \dots A_n \rangle_\rho = \text{Tr}(\rho A_1 \dots A_n). \quad (1.20)$$

It is worth to comment here that the expression (1.20) does not hold true if the measurements are not compatible. The mean values for non-compatible measurements performed in sequence should take into account the post-measurement state as described in the Born's rule (11) and the expression for the mean value turns out to be different. In the case of two measurements performed in sequence, first A_1 and then A_2 , the mean value is:

$$\langle A_1 A_2 \rangle_\rho = \frac{1}{2} \text{Tr}(\rho \{A_1, A_2\}). \quad (1.21)$$

Given the set of rules about how to describe quantum states, quantum measurements, relations of compatibility between measurements and the Born's rule, we can now move on to showing that quantum theory is a contextual theory.

1.3 Quantum theory as a contextual theory

In what follows we will present two different approaches to prove that quantum theory is contextual. First, in Sec. 1.3.1, we provide an example of a state in a three-dimensional Hilbert space and a set

of measurements that violate the KCBS inequality stated in Eq. (1.5); this is the simplest example known in the literature. Then, in Sec. 1.3.2 we show that there are sets of quantum measurements that do not simultaneously admit deterministic assignments of outcomes; this property is usually referred to as state-independent quantum contextuality because it concerns only sets of measurements, not quantum states.

1.3.1 State-dependent quantum contextuality

For convenience, let us state here again the KCBS inequality together with the corresponding classical bound derived already in Sec. 1.3.1,

$$I_{KCBS} := \langle A_0 A_1 \rangle + \langle A_1 A_2 \rangle + \langle A_2 A_3 \rangle + \langle A_3 A_4 \rangle - \langle A_4 A_0 \rangle \leq \eta^C = 3. \quad (1.22)$$

Let us then consider the following one-qutrit state

$$|\psi\rangle = |0\rangle \equiv (1, 0, 0)^T \quad (1.23)$$

as well as five observables defined as

$$A_i = 2|v_i\rangle\langle v_i| - \mathbb{1}, \quad (1.24)$$

where $|v_i\rangle$ are three-dimensional real vectors given by

$$|v_i\rangle = (\cos \theta, \sin \theta \sin \phi_i, \sin \theta \cos \phi_i)^T, \quad (1.25)$$

where θ is defined as $\cos \theta = \sqrt{1/(1+2\alpha)}$ with

$$\alpha = \frac{1}{2} \sec\left(\frac{\pi}{3}\right) \quad (1.26)$$

and

$$\phi_i = \frac{2}{3}\pi i. \quad (1.27)$$

It is not difficult to verify that $\langle v_i | v_{i+1} \rangle = 0$ for $i = 0, \dots, 4$ and therefore the pairs of observables A_i and A_{i+1} commute, that is, $[A_i, A_{i+1}] = 0$. In this way, we certify that this quantum realization actually fits the compatibility structure of the KCBS scenario as described in the Sec. 1.1 and pictured in Fig. 1.1. Fig. 1.2 illustrates this quantum realization geometrically. After calculating the expectation values for the compatible pairs of measurements, it can be checked that

$$I_{KCBS} := \langle A_0 A_1 \rangle + \langle A_1 A_2 \rangle + \langle A_2 A_3 \rangle + \langle A_3 A_4 \rangle - \langle A_4 A_0 \rangle = \frac{3 \cos(\pi/5) - 1}{1 + \cos(\pi/5)} 5 \cong 3.9. \quad (1.28)$$

We thus conclude that the above three-dimensional quantum realization violates the noncontextuality inequality (1.5). In this sense quantum theory is contextual.

It is important to notice that the value of I_{KCBS} in Eq. (1.28) is the maximal one that I_{KCBS} can achieve in quantum theory [10]. Apart from this, the above quantum realization is unique up to an arbitrary unitary transformation. This fact motivates exploiting quantum contextuality for the purpose of certification of quantum states and measurements and actually underlies the concept of contextuality-based self-testing of quantum systems we exploit in this thesis (see Sec. 1.6 for a rigorous

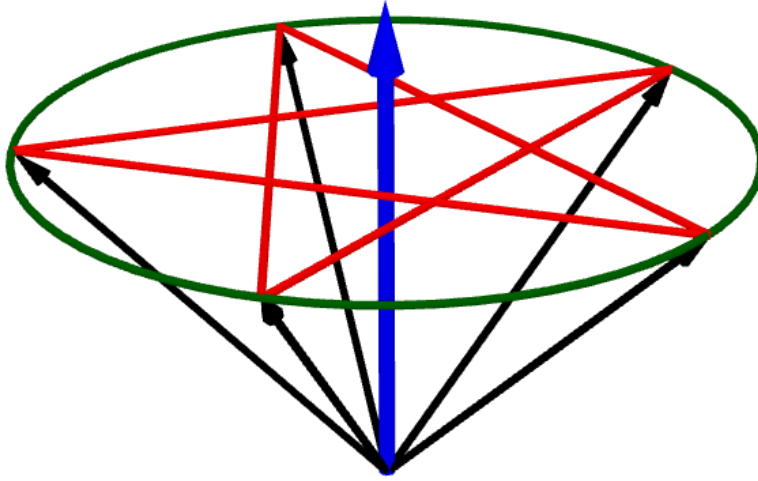


Figure 1.2: Geometrical representation of a quantum realization that violates maximally the KCBS inequality. The blue vector represents the quantum state (1.23) whereas the black vectors represent the vectors (1.25) defining the five measurements.

definition of self-testing).

In the previous sections, we explained that the sets of classical probabilities as well as those respecting the non-disturbance condition, are both polytopes in the space of correlations. Let us now comment on the set of quantum correlations, i.e., correlations that are obtained by performing quantum measurements on quantum states, and also discuss its relation to the previous two sets (see Fig. 1.3).

The first thing to take into account is that the set of probabilities that are described by quantum theory is convex, given that we do not impose any constraints on the dimension of the underlying Hilbert space, i.e., any convex combination of probability distributions achievable within quantum theory gives rise to another quantum realization [31], which, however, might be defined in a higher-dimensional Hilbert space. The second point here is that while any probability distribution admitting the NCHV model (1.3) can be reproduced by quantum theory with a convenient choice of compatible measurements and a quantum state, the quantum set contains behaviors \vec{p} such as for instance the one presented above that cannot be reproduced by the NCHV models. So the classical polytope is a proper subset of the convex quantum set. At the same time, it is not difficult to verify that quantum correlations respect the non-disturbance condition, and hence the quantum set belongs to the non-disturbance polytope.

Let us finally notice that both the CHSH and the KCBS inequalities are particular examples belonging to a family of noncontextual inequalities, usually referred to as n -cycle inequalities ($n \geq 4$), which are of the following form

$$I_{n\text{-cycle}} := \sum_{i=0}^{n-1} \gamma_i \langle A_i A_{i+1} \rangle \leq \eta^C = n - 2, \quad (1.29)$$

where $\gamma_i \in \{-1, 1\}$ and the number of negative coefficients γ_i is odd. Notice that the graphs of com-

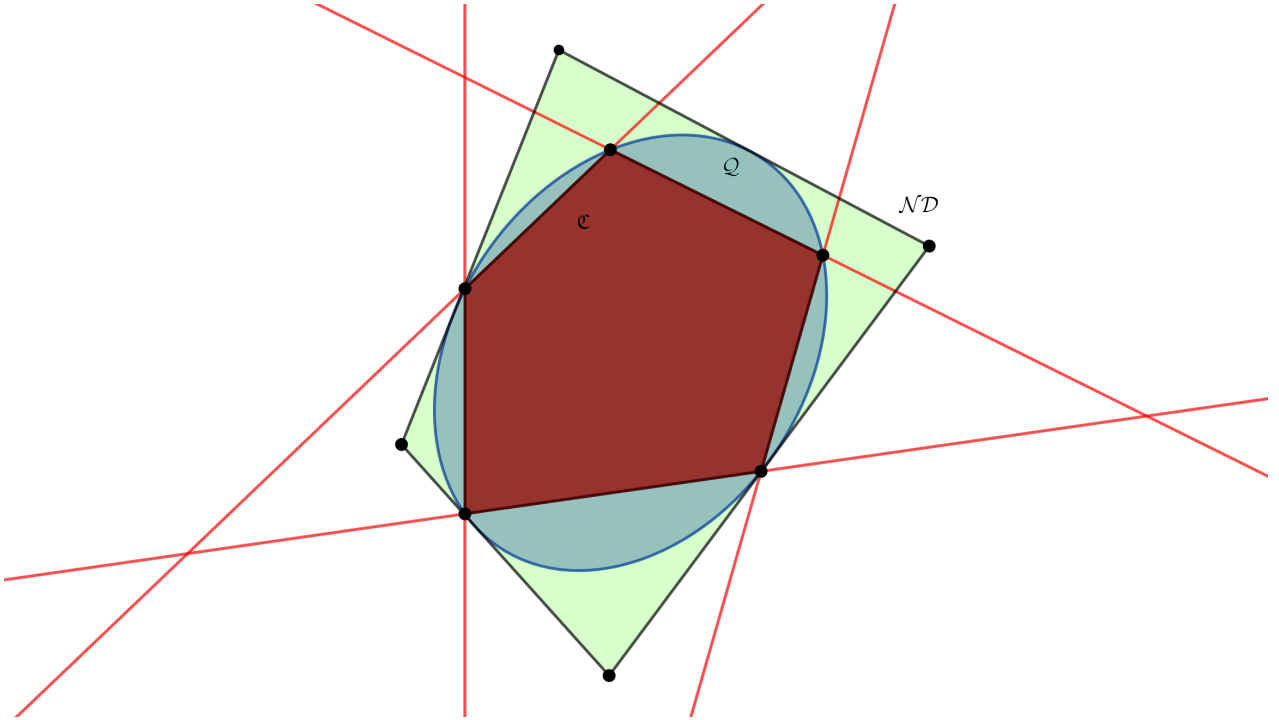


Figure 1.3: **Pictorial representation of the set of probabilities.** The classical polytope \mathcal{C} is contained in the convex quantum set \mathcal{Q} which in turn is contained in the non-disturbance polytope \mathcal{ND} . The red straight lines represent the noncontextuality inequalities characterizing the classical polytope in the set of probabilities.

patibility for the CHSH and the KCBS scenarios presented in Fig. 1.1 are n -cycles for $n = 4$ and $n = 5$, respectively. In this most general scenario, the contexts are given by the pairs of measurements A_i and A_{i+1} , i.e., $[A_i, A_{i+1}] = 0$ with the sum modulo n and all the measurements have two outcomes ± 1 . The quantum bound for this inequality is known to be [32]

$$\eta_Q^n = \begin{cases} \frac{3n \cos(\pi/n) - n}{1 + \cos(\pi/n)}, & \text{if } n \text{ is odd} \\ n \cos(\pi/n), & \text{if } n \text{ is even} \end{cases} \quad (1.30)$$

The quantum bound for odd n is attained in a three-dimensional Hilbert space and the corresponding set of measurements has a quite similar geometric structure to the set of measurements that gives rise to the maximal violation of the KCBS inequality. On the other hand, for even n , the quantum realization attaining η_Q^n lives in a four-dimensional Hilbert space. The Reader is referred to [32] for more details about the n -cycle inequalities.

As for the CHSH Bell inequality, we provide a quantum realization maximally violating it later in Sec. 1.5, where we also introduce composite quantum systems and discuss that nonlocality is a special case of quantum contextuality.

1.3.2 State-independent quantum contextuality

In this subsection we show further interesting examples of quantum contextuality, which are independent of quantum states. One of the most peculiar features about quantum contextuality is that there are special sets of measurements that cannot be jointly assigned to deterministic outcomes. One of the

most intriguing interpretations of this feature is that the measurement does not reveal a pre-defined outcome that is independent of any other compatible measurement performed on a quantum system.

The first example in the literature that shows the existence of state-independent quantum contextuality is due Kochen and Specker [7]. The theorem proven by these authors is a “no-go” theorem. In this proof they exhibited a set of 117 rank-one projectors acting on $\mathcal{H} = \mathbb{C}^3$ that obey certain orthogonality relations, and showed that it is impossible to simultaneously assign deterministic outcomes to all of the associated measurements. Other such proofs with less rank-one projections or measurements can be found in Refs. [33]-[34]-[35]-[36].

Another example is the Peres-Mermin square [37]-[38] which is one of the simplest proofs of state-independent quantum contextuality. It consists of nine measurements, which we denote here by M_{ij} with $i, j \in \{1, 2, 3\}$, all of them have two outcomes, labelled by 1 and -1 . The measurements are organized into a 3×3 square in such a way that the measurements belonging to its rows and columns form six contexts [see Fig. 1.4]. Finally, the measurements are assumed to satisfy a set of conditions:

$$M_{i1}M_{i2}M_{i3} = \mathbb{I} \quad (i = 1, 2, 3), \quad (1.31)$$

$$M_{1i}M_{2i}M_{3i} = \mathbb{I} \quad (i = 1, 2) \quad (1.32)$$

and

$$M_{13}M_{23}M_{33} = -\mathbb{I}. \quad (1.33)$$

In other words, the product of the observables forming each context is the identity except for the last column for which it is $-\mathbb{I}$. It turns out that the simplest quantum realization of the measurements M_{ij} satisfying all the above requirements is given by

$$\begin{aligned} M_{11} &= X \otimes \mathbb{I}, & M_{12} &= \mathbb{I} \otimes X, & M_{13} &= X \otimes X, \\ M_{21} &= \mathbb{I} \otimes Z, & M_{22} &= Z \otimes \mathbb{I}, & M_{23} &= Z \otimes Z, \\ M_{31} &= X \otimes Z, & M_{32} &= Z \otimes X, & M_{33} &= Y \otimes Y, \end{aligned} \quad (1.34)$$

where X, Y and Z are the qubit Pauli matrices. At the same time it is impossible to find nine classical variables taking values ± 1 that would satisfy the above constraints, which proves quantum theory to be a contextual theory.

1.4 Quantum theory as a nonlocal theory

This part is dedicated to composite systems, which are systems composed of many systems (referred to as subsystems) that are spatially separated. We will explain here the notions of a Bell scenario and Bell nonlocality which can be seen as a particular case of contextuality for composite systems in which compatibility of measurements is guaranteed by spatial separation. In fact, historically, the concept of Bell non-locality was developed first [2] and only later generalized to quantum contextuality [7].

We begin by illustrating the Bell scenario in the simplest possible case. To this end, we consider a system, be it classical, quantum or even one falling in the framework of GPTs, which is composed of two spatially separated subsystems that are distributed among two parties, named Alice and Bob. Let us

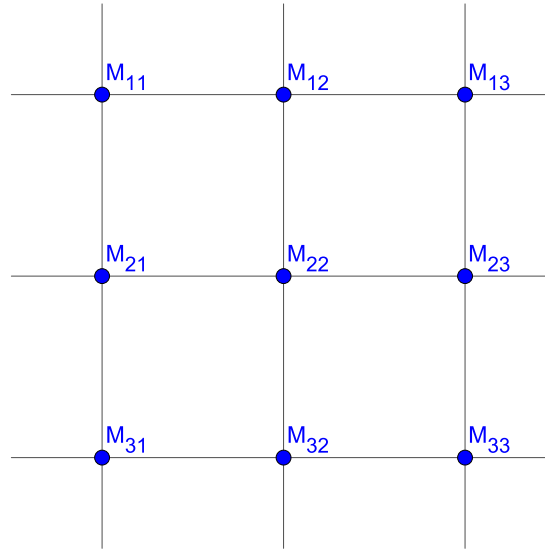


Figure 1.4: **The Peres-Mermin square.** In this graph, the vertices represent the measurements M_{ij} and the lines the contexts. The product of the Hermitian operators associated to the same line always equals \mathbb{I} , except for the third vertical line, for which it is $-\mathbb{I}$. This leads to a contradiction when trying to simultaneously assign a classical deterministic strategy to the outcomes of all the nine measurements and it is one of the simplest proofs of state-independent quantum contextuality.

then assume that both parties can freely choose to perform one of two measurements on their systems; Alice's and Bob's measurements are denoted A_i and B_j , respectively. Each of these four measurements has two outcomes and we label them by ± 1 . Fig. 1.5 depicts this bipartite Bell scenario.

As already outlined in Sec. 1.1, the correlations generated in this experiment are described by a collection of probability distributions $\vec{p} = \{p(a, b | A_i, B_j)\}$, where a and b stand for the outcomes of Alice and Bob, respectively. For composite systems a non-contextual hidden variable model introduced in Sec. 1.1 in which compatibility of measurements is guaranteed by spacial separation is referred to as a local hidden variable model. The non-disturbance condition within the framework of Bell scenario is then referred to as the non-signalling condition which says that information cannot be transmitted between separated systems at arbitrary speed.

Since there is a spatial separation between Alice's and Bob's laboratories, they can perform the local measurements instantaneously in a such way that there is no way of classical communication between them as represented in Fig. 1.6; in other words, one event in the space-time does not belong to the light cone of the other event. Hence, we can consider the measurements performed in different locations as compatible.

Let us now show that quantum theory is nonlocal in the sense that it gives rise to correlations \vec{p} which violate Bell inequalities. Before doing that we need, however, to introduce the description of composite system within the framework of quantum theory, concentrating on the simplest bipartite systems; it is direct to generalize what follows to systems consisting of an arbitrary number of components. For this purpose, we consider two systems A and B which are described by Hilbert spaces \mathcal{H}_A and \mathcal{H}_B . Then, the joint system is represented by a Hilbert space which is a tensor product of the

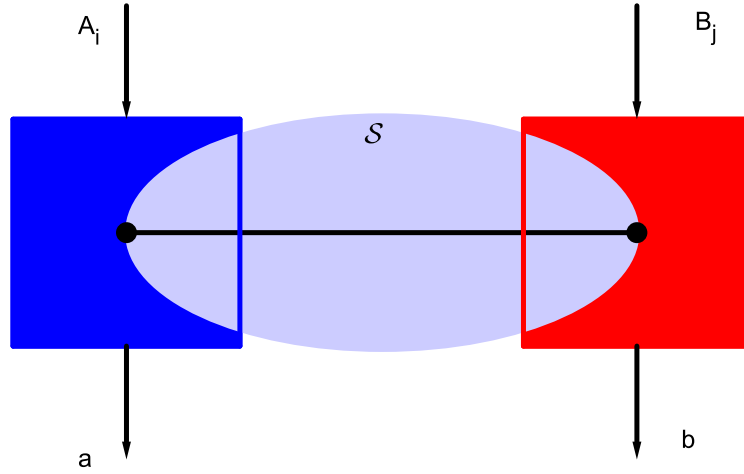


Figure 1.5: Representation of a bipartite Bell scenario. This scenario comprises a state \mathcal{S} which is shared between two labs. In each lab Alice and Bob can perform instantaneously the measurements A_j and B_j respectively, where $i, j \in \{0, 1\}$. Each measurement have 2 outcomes, labelled by a, b where $a, b \in \{-1, 1\}$. After many runs of a experiment, the probabilities $p(a, b|A_i, B_j)$ can be calculated as well the expectation values $\langle A_i B_j \rangle$.

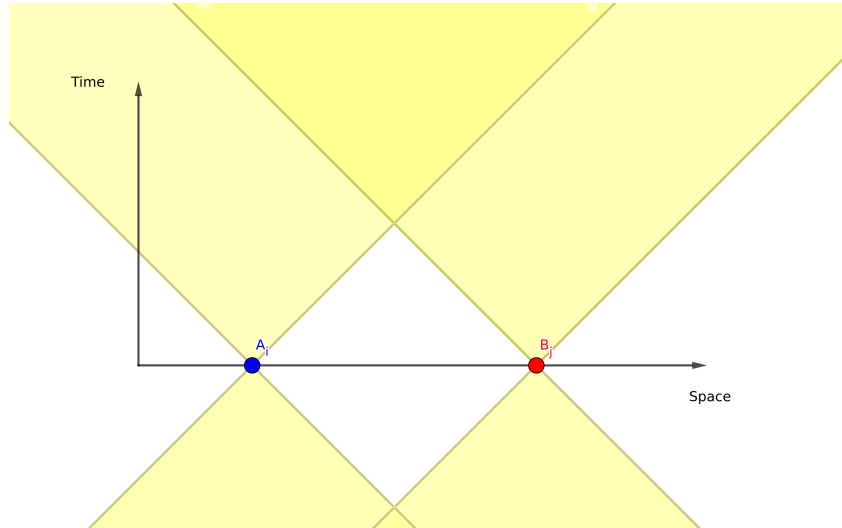


Figure 1.6: This figure represents the light's cone of the events associated to the local measurements of Alice and Bob on a quantum state shared by them. Let us observe that one event does not belong to the light's cone of another one. In the inertial referential showed, both events happen simultaneously and thus there is no way that one event influences the outcome of the other event. This means that the measurements performed by Alice and Bob can be considered compatible.

local ones,

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B. \quad (1.35)$$

Recall that a tensor product of Hilbert spaces \mathcal{H}_i is also a Hilbert space defined as a linear span of all vectors belonging to both \mathcal{H}_A and \mathcal{H}_B , and its dimension is simply a product of the dimensions of the local spaces, i.e., $\dim \mathcal{H} = \dim \mathcal{H}_A \cdot \dim \mathcal{H}_B$.

In particular, to construct a basis of \mathcal{H} it is enough to take a tensor product of bases of the local Hilbert spaces. To illustrate this with an example, let us consider the case where $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = 2$ and let us take the local orthonormal bases to be simply the computational ones: $\mathcal{H}_A = \text{span}\{|0\rangle_A, |1\rangle_A\}$ and $\mathcal{H}_B = \text{span}\{|0\rangle_B, |1\rangle_B\}$. Then,

$$\mathcal{H} = \text{span}\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\}. \quad (1.36)$$

In what follows, for simplicity, we denote the tensor product by $|i\rangle_A \otimes |j\rangle_B = |ij\rangle$. Interestingly, the structure of the joint Hilbert space \mathcal{H} is much richer than can be naively inferred from its definition because apart from the simple vectors given in Eq. (1.36), it contains also pure states which cannot be expressed as a tensor product of pure states belonging to the local Hilbert spaces. Such states are called entangled [cf. Sec. 1.5] and a celebrated example of such a state is one that has found numerous applications within the field of quantum information, for instance, in quantum quantum teleportation [39] or quantum cryptography [15], and is typically referred to as the maximally entangled state of two-qubits:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (1.37)$$

Let us finally discuss the measurements. Suppose that on their local systems one of the parties, say Alice, performs a measurement represented by an observable A . Then, the associated operator acting on the joint system is $A \otimes \mathbb{I}$. In an analogous way one represents the measurements of Bob. If, moreover, Alice and Bob perform these measurements simultaneously, the associated Hermitian operator is $A \otimes B$. Given the description of the state and measurements, the Born's rule (11) to calculate the probabilities and the state after the measurements follow straightforwardly.

We are now ready to show that quantum theory is nonlocal. With this purpose, we focus our attention to the CHSH Bell inequality (1.4) and assume that Alice and Bob now share the two-qubit maximally entangled state (1.37) and measure on their local systems the following observables:

$$A_0 = X, \quad B_0 = \frac{X + Z}{\sqrt{2}}, \quad (1.38)$$

$$A_1 = Z, \quad B_1 = \frac{X - Z}{\sqrt{2}}. \quad (1.39)$$

After some calculations one finds that the value for the CHSH expression amounts to

$$I_{\text{CHSH}} := \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle = 2\sqrt{2}, \quad (1.40)$$

which clearly exceeds the maximal value of I_{CHSH} over NCHV models which is 2. Importantly, the value $2\sqrt{2}$ in (1.40) is the maximal one that I can reach within quantum theory [40], [41], and, moreover, the quantum state (1.37) and measurements (1.38) giving rise to this maximal value are unique up to certain well-known equivalences. This fact lies at the heart of self-testing schemes, which are used

for certification of quantum systems based on the observed nonclassical correlations [17] (see also Sec. 1.6). In Chapter 4 we provide a general construction of Bell inequalities that are maximally violated by multipartite graph states of arbitrary prime local dimension and show that in the particular case of qutrit systems, the obtained Bell inequalities can be used for self-testing.

It is worth commenting here that extensions of this scenario to situations involving more observers, measurements, or outcomes can be done naturally, and there are many results in the literature studying such generalizations [42]–[46].

1.5 Entanglement

Entanglement is a crucial concept in quantum theory. It contains a basic notion of nonclassicality for composite systems and it is also a key feature of quantum theory enabling Bell nonlocality. First, we introduce a formal definition of a separable and entangled states:

Definition 13 (Bipartite separable and entangled states). *A pure bipartite state $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if it can be written as a tensor product of pure states describing each subsystem, that is, $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$. On the other hand, $|\psi_{AB}\rangle$ is called entangled if it is not separable.*

In order to continue the discussion about entanglement, let us consider a simple example of a pure entangled state composed of two qubits:

$$|\psi\rangle = \alpha|00\rangle + \beta|11\rangle, \quad (1.41)$$

where α, β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$ and $\alpha, \beta \neq 0$. Notice that the entangled state (1.37) that maximally violates a Bell inequality is a particular case when $\alpha = \beta = \frac{1}{\sqrt{2}}$.

Any pure two-qubit state which is separable can be written as:

$$|\phi_1\rangle \otimes |\phi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle, \quad (1.42)$$

where $|\phi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\phi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ are local normalized vectors. After comparing Eqs. (1.41) and (1.42), one sees that

$$|\psi\rangle = \alpha|00\rangle + \beta|11\rangle \neq |\phi_1\rangle \otimes |\phi_2\rangle \quad (1.43)$$

because the equations $\alpha_1\beta_2 = \beta_1\alpha_2 = 0$, $\alpha_1\alpha_2 = \alpha$ and $\beta_1\beta_2 = \beta$ cannot be simultaneously satisfied for $\alpha, \beta \neq 0$. Trivial examples of separable states are for instance the elements of the product basis which spans the two-qubit Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$, i.e., $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. On the other hand, the four states defined below,

$$|\psi_{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \quad |\phi_{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}, \quad (1.44)$$

which are usually called the Bell states, are all entangled, and also span $\mathbb{C}^2 \otimes \mathbb{C}^2$. The Bell states, are examples of the maximally entangled states of two qubits. On the other hand, for all values of α and β such that $|\alpha| \neq |\beta|$ and $\alpha, \beta \neq 0$ the state (1.41) is non-maximally entangled.

Some interesting behaviors happen in composite systems when the shared state is pure and entangled. In order to support this statement let us assume that a Bell state is shared between Alice and Bob. If Alice performs the local measurement associated with the Pauli matrix Z , after collecting the result of the outcome, she knows the updated state and, consequently, she knows instantaneously the outcome of the measurement Z performed locally by Bob independently of the distance between them. At first sight, we could think that this would violate the basic principle in nature that information can be transmitted only with finite speed, however, Alice does not have control of any information that could be sent to Bob. It is like the famous "spooky action at a distance" pointed out in the EPR paradox [1]. The properties of quantum theory like this one are at the heart of quantum information protocols such as quantum teleportation [39], [47], [48], entanglement distillation [49], [50], quantum cryptography [51] and quantum computing [52], [53].

Let us also briefly discuss the notion of multipartite entanglement, which corresponds to a situation in which a quantum system at hand consists of more than two subsystems. Analogously to the bipartite case, a multipartite pure state is called entangled if it cannot be written as a tensor product of pure state describing individual subsystems. An example of a multipartite entangled state is the N -qubit Greenberger–Horne–Zeilinger (GHZ) state:

$$|\text{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}), \quad (1.45)$$

where N is an arbitrary integer such that $N \geq 2$. Following the same reasoning as above, it is not difficult to show that this state cannot be written as a tensor product of local states, so it is entangled.

While in the case of the pure states we discussed here, i.e. (1.41) and (1.45), it was not difficult to show that they are entangled, the problem of deciding whether an arbitrary mixed quantum state is entangled or not is a highly non-trivial task; in fact, as shown in Ref. [54], this is an NP-hard problem. It is worth mentioning here that nevertheless there exist methods to detect entanglement of quantum states such as the one based on partial transposition [55] (see also the review [56] for other methods of entanglement detection).

A point we have to comment on here also is the relation of entanglement with Bell nonlocality. If a state is separable, it will not violate any Bell inequality, so entanglement is a necessary resource for nonlocality. In fact, any state that exhibits nonlocality in the sense that it violates some Bell inequality is entangled. However, the opposite implication is in the general mixed-state case not true as there exist entangled states which do not violate Bell inequalities [57]. Moreover, if the local measurements at Alice's or Bob's sides commute, it is again impossible to violate a Bell inequality; in particular, in the case of the CHSH Bell inequality, one can verify that the local measurements given in Eq. (1.38) do not commute. Let us finally mention that as proven in a series of papers [40], [41], [58], [59] the maximal quantum violation of the CHSH inequality can be achieved if, and only if the underlying state and measurements are equivalent, under certain well-defined equivalences, to the maximally entangled state of two qubits (1.37) and the particular Pauli measurements specified in Eqs. (1.38) and (1.39). This form of uniqueness of the quantum realization giving rise to the maximal violation of Bell inequalities is the key fact behind the notion of self-testing (see Sec. 1.6 for a definition) which is a central concept in this thesis.

1.5.1 Graph states

Let us now introduce the definition of graph states of arbitrary prime local dimension [60]-[61]. This is a particular class of multipartite entangled quantum states that has found numerous applications in quantum information processing. For instance, the cluster states, which are a particular instance of graph states, are a key resource for a scheme of one-way quantum computing [52]-[53]. Then, some constructions for quantum error-correction codes are based on them [60]-[62] and they find applications in quantum cryptography [63]. Finally, graph states exhibit non-local properties [64] and can be self-tested [65]-[22]. Apart from that, graph states have a very convenient mathematical representation which is helpful in designing certification methods for them. For both these reasons graph states are studied in this thesis.

Consider a weighted graph $\mathcal{G} = (\mathcal{V}, \mathcal{R}, d)$, where $\mathcal{V} := \{1, \dots, N\}$ is the set of vertices and $\mathcal{R} := \{r_{ij}\}$ is the set of integer numbers from the set $\{0, \dots, d-1\}$ specifying the weights of the edges between the vertices $i, j \in \mathcal{V}$; in the particular case of $r_{ij} = 0$ there is no edge connecting vertices i and j . We additionally assume that $r_{ii} = 0$ for each i , that is, there are no loops in the graph and that $r_{ij} = r_{ji}$, i.e., the edges are symmetric between themselves. Throughout this thesis we assume d to be prime and the graph to be connected meaning that there exists a path between every pair of vertices.

Let us now show how to use graphs to construct pure quantum states. To this aim, we assume that each vertex of \mathcal{G} corresponds to a single d -dimensional subsystem of an N -partite quantum system, where as already stated d is a prime number such that $d \geq 2$. To each vertex $i \in \mathcal{V}$ of the graph we then associate a stabilizing operator defined as,

$$G_i = X_i \otimes \bigotimes_{j \neq i} Z_j^{r_{ij}}, \quad (1.46)$$

where X, Z are the generalizations of the qubit Pauli matrices to the d -dimensional Hilbert spaces defined in Eq. (1.10), and r_{ij} are powers of the Z operator. Then, the graph state corresponding to the graph \mathcal{G} is defined in the following way:

Definition 14. We define the qudit graph state $|G\rangle$ associated to the weighted graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, d)$ to be the unique normalized vector from $(\mathbb{C}^d)^{\otimes N}$ stabilized by the corresponding operators G_i (1.46), that is,

$$\forall i = 1, \dots, N \quad G_i |G\rangle = |G\rangle. \quad (1.47)$$

In other words, $|G\rangle$ is the unique common eigenstate of all operators G_i corresponding to the eigenvalue $+1$.

It is worth noting that the stabilizing operators (1.46) mutually commute and the Abelian group generated by them, being a subgroup of the N -qudit Pauli group, is called a stabilizer. In fact, the above definition of graph states falls within the stabilizer formalism which is known for its use in quantum error correction [66]. The latter is a very convenient way of representing multipartite entangled quantum states or even entangled subspaces and thus is another central concept in this thesis.

In the qubit case, when $d = 2$, the weights r_{ij} take only two values, zero or one, corresponding to the absence or presence of an edge between vertices i and j . Thus, for simplicity, we denote the graph by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where, \mathcal{E} is the set of edges connecting vertices. In this case, we also denote by $\mathcal{N}(i)$



Figure 1.7: The simplest connected graph giving rise to bipartite maximally entangled states such as the one in Eq. (1.37).

the neighborhood of the vertex i , i.e., the subset of vertices which are connected to the vertex i by an edge and the definition of the stabilizing operators is given by

$$G_i = X_i \otimes \bigotimes_{j \in \mathcal{N}(i)} Z_j, \quad (1.48)$$

where X, Z are the qubit Pauli matrices and the definition of the qubit graph states is just a particular case of Def. 14.

Let us now introduce a few examples of graph states in the simplest case of $d = 2$. The simplest graph is the one that consists of two connected vertices [cf. Fig. 1.7]. The stabilizing operators associated to this graph are given by:

$$G_1 = X \otimes Z, \quad G_2 = Z \otimes X. \quad (1.49)$$

Let us now use this example to exhibit the self-consistence of the definition of graph states through the stabilizer formalism. We will show that there exist a unique eigenvector with eigenvalue 1 of both stabilizing operators in Eq. (1.49). Each of them is a Hermitian operator with eigenvalues ± 1 , where each eigenvalue is doubly-degenerate. The eigenspaces of G_1 and G_2 corresponding to the eigenvalue 1 are, respectively, $\text{span}\{|+0\rangle, |-1\rangle\}$ and $\text{span}\{|0+\rangle, |1-\rangle\}$. The intersection of these two subspaces is one-dimensional subspace spanned by $(1/\sqrt{2})(|+0\rangle + |-1\rangle)$. So, the unique (up to a global phase) common eigenstate with eigenvalue 1 of both stabilizing operators is $|G_1\rangle = (1/\sqrt{2})(|+0\rangle + |-1\rangle)$, which is equivalent to the maximally entangled state of two qubits up to a local unitary.

The other two examples of connected graphs with three vertices are depicted in Fig. 1.8. The graph on the left side is complete, i.e., every pair of vertices in it is connected by an edge. The unique three-qubit state associated to this graph is stabilized by the following three stabilizing operators

$$G_1 = X \otimes Z \otimes Z, \quad G_2 = Z \otimes X \otimes Z, \quad G_3 = Z \otimes Z \otimes X, \quad (1.50)$$

and its explicit form reads

$$|G_2\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |100\rangle + |010\rangle - |110\rangle + |001\rangle - |101\rangle - |011\rangle - |111\rangle). \quad (1.51)$$

The graph on the right side in Fig. 1.8 is another three-vertex graph which is not isomorphic to the complete graph. The unique three qubit state associated with this graph is stabilized by

$$G_1 = X \otimes Z \otimes Z, \quad G_2 = Z \otimes X \otimes \mathbb{I}, \quad G_3 = Z \otimes \mathbb{I} \otimes X, \quad (1.52)$$

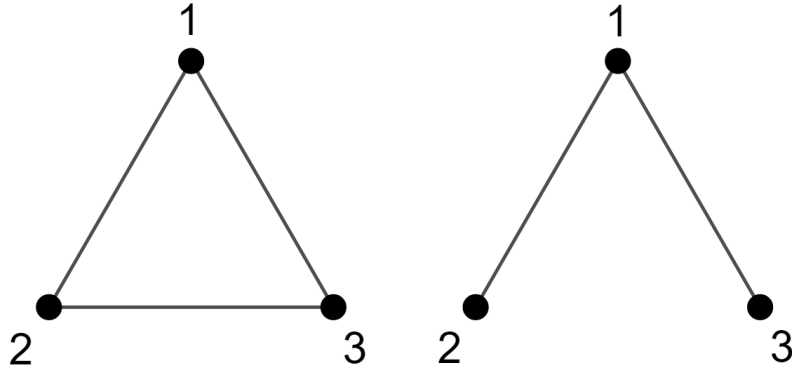


Figure 1.8: Two non-isomorphic graphs with 3 vertices. On the left side a complete graph and on the right side another three-vertex graph which is inequivalent to the first one.

and is given by

$$|G_3\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |100\rangle + |010\rangle - |110\rangle + |001\rangle + |101\rangle - |011\rangle + |111\rangle). \quad (1.53)$$

Interestingly, although both these states $|G_2\rangle$ and $|G_3\rangle$ correspond to non-isomorphic graphs, they are actually equivalent to the same three-qubit GHZ state

$$|\text{GHZ}_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad (1.54)$$

up to local unitary transformations.

Let us finally provide an alternative definition of the graph states, which exhibits how these states can be implemented, for instance on a quantum computer [cf. Ref. [67]]:

$$|G\rangle = \prod U_{ab}^{r_{ab}} |+\rangle^{\otimes N}, \quad (1.55)$$

where $|+\rangle$ is the eigenstate of the Pauli matrix X and U_{ab} is a unitary matrix raised to the power r_{ij} that acts on qubits a and b , and it is given by the following expression:

$$U_{ab} = |0\rangle_a \langle 0| \otimes I_b + |1\rangle_a \langle 1| \otimes Z_b + \dots + |d-1\rangle_a \langle d-1| \otimes Z_b^{d-1} = \sum_{m=0}^{d-1} |m\rangle_a \langle m| \otimes Z_b^m. \quad (1.56)$$

For the qubit case, the matrix U_{ab} is given by:

$$U_{ab} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = |0\rangle_a \langle 0| \otimes I_b + |1\rangle_a \langle 1| \otimes Z_b, \quad (1.57)$$

which is also known as the controlled Z gate. A suitable comment here is that $U_{ab} = U_{ba}$, as can be checked, and that all of these unitary transformations acting in different vertices commute among

themselves, i.e., $[U_{ab}, U_{cd}] = 0$ for all vertices denoted by $a \neq b$ and $c \neq d$. As a consequence, the ordering of the unitaries in the usual matrix product plays no role in the definition (1.56) and therefore the graph states are well defined since the graph does not distinguish edges between different vertices.

This alternative definition brings interesting physical interpretations of graph states. To prepare a graph state, for instance, we could start with the state which is a tensor product of eigenstates of the qubit Pauli matrix X , i.e. $|+\rangle^{\otimes N}$, and then apply the non-local unitaries U_{ab} which create entanglement in the state. The initial state can be for instance obtained by preparing each qubit in the ground state $|0\rangle$ and applying the Hadamard gate to it, whereas the action of the non-local unitaries can be implemented by a suitable Hamiltonian acting on pairs of qubits.

In summary, while the second definition of the graph states provides also a recipe of how to physically generate these states, the definition based on the stabilizer formalism is a convenient mathematical tool that allows us to design certification methods for them and thus is highly relevant for the thesis. More details about entanglement in graph states can be found in the review [67].

1.6 Self-testing

Self-testing is one of the strongest forms of device-independent certification whose main goal is to exploit the observed non-classical correlations to deduce the form of the quantum state and measurements that gave rise to these correlations [17] (see also the recent review [18]). Self-testing is thus of black box type certification method that allows making nontrivial statements about the underlying quantum system from the violation of Bell or noncontextuality inequalities without making assumptions on the system. The main idea behind the proofs of self-testing lies in the uniqueness (up to certain equivalences) of the quantum realization that attains the maximal quantum violation of some inequalities such as the CHSH or the KCBS inequalities described above.

Below follows a formal definition of self-testing based on violation of noncontextuality inequalities that was first put forward in Ref. [68]. We use this definition later in Chapters 2 and 3.

Definition 15 (Self-testing from contextuality). *Suppose an unknown state $|\psi\rangle \in \mathcal{H}$ and a set of measurements A_i violate a given noncontextuality inequality maximally, then this maximal quantum violation self-tests the state $|\tilde{\psi}\rangle \in \mathbb{C}^d$ and the set of measurements \tilde{A}_i if there exists a projection $P: \mathcal{H} \rightarrow \mathbb{C}^d$ and a unitary U acting on \mathbb{C}^d such that*

$$U^\dagger(PA_iP^\dagger)U = \tilde{A}_i \quad (1.58)$$

$$U(P|\psi\rangle) = |\tilde{\psi}\rangle. \quad (1.59)$$

Let us also state the definition of self-testing in the case of Bell scenarios which historically was in fact introduced earlier than the above one. For pedagogical reasons we provide it for bipartite scenarios, noting that the generalization to the multipartite case can straightforwardly be obtained by adding more observers. Also, we formulate it in a slightly different manner as compared to the original one [69] because we use unitary operations instead of isometries.

Definition 16 (Self-testing from nonlocality - bipartite Bell scenario). *Let us suppose that a bipartite Bell test is performed on an unknown state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and with unknown measurements A_i ($A_i: \mathcal{H}_A \rightarrow \mathcal{H}_A$) and B_j ($B_j: \mathcal{H}_B \rightarrow \mathcal{H}_B$). We say that the observed correlations \vec{p} self-test the state $|\tilde{\psi}\rangle \in$*

$\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ and the measurements \tilde{A}_i and \tilde{B}_j if one can prove that: (i) the local Hilbert spaces \mathcal{H}_A and \mathcal{H}_B decompose as $\mathcal{H}_A = \mathbb{C}^{d_A} \otimes \mathcal{H}'_A$ and $\mathcal{H}_B = \mathbb{C}^{d_B} \otimes \mathcal{H}'_B$, (ii) there exist local unitary operations U_A and U_B such that

$$U_A \otimes U_B |\psi\rangle = |\tilde{\psi}\rangle \otimes |\text{aux}\rangle \quad (1.60)$$

for some auxiliary state $|\text{aux}\rangle \in \mathcal{H}'_A \otimes \mathcal{H}'_B$ and, moreover,

$$U_A^\dagger A_i U_A = \tilde{A}_i \otimes \mathbb{I}, \quad U_B^\dagger B_j U_B = \tilde{B}_j \otimes \mathbb{I}. \quad (1.61)$$

We remark that compared to the definition stated for self-testing based on noncontextuality inequalities, the definition used for Bell nonlocality does not use any projection operator. The difference remains in the fact that the projectors in the first definition discard the auxiliary Hilbert Space. Both definitions are different points of view of similar mathematical structures.

A simple example of an inequality useful for certification purposes is the CHSH inequality [40]–[70]. Its maximal violation self-tests, up to the equivalences specified in the above definition, the maximally entangled state of two qubits (1.37) and four measurements (1.38)–(1.39), which locally anti-commute. Thus, this quantum realization is the unique one in the two-qubit Hilbert space that up to local unitary operations attains the maximal quantum violation of the CHSH Bell inequality. This is the first example in the literature about a certification scheme based on maximal violation of a Bell inequality and since then self-testing schemes for other quantum states have been proposed (see, e.g., [19]–[24]). Our thesis fits this line of research. In fact, in Chapter 4 we present the article with a self-testing result for qutrit graph states [71].

Another example of an inequality that self-tests a quantum system is the KCBS inequality (1.22). The quantum realization we described in section (1.3.1) is, up to a unitary equivalence, the unique one in $\mathcal{H} = \mathbb{C}^3$ that gives rise to the maximal violation of this inequality, up to a global unitary [25]. As already mentioned self-testing methods based on Bell inequalities are device-independent as they do not depend on any assumption on the state and measurements. In a Bell test, the fact that the measurements performed by different observers commute is guaranteed by spatial separation. At the same time, it is worth mentioning that the assumption of commutativity of measurements is a weakness of self-testing schemes based on noncontextuality inequalities. It was one of the main aims of this thesis to provide a method allowing to certify the quantum realizations giving rise to the maximal violation of the KCBS or the n -cycle inequalities without assuming the compatibility structure of the underlying measurements. In fact, in Chapter 2 we present a scheme based on sequential measurements which allows one to drop the assumption of commutativity between measurements [72]. Then, in Chapter 3 we present a self-testing scheme based on the standard contextuality scenario [73].

Let us notice that to provide a self-testing scheme for a particular quantum realization one typically follows a similar strategy which consists of constructing a non-trivial Bell or noncontextuality inequality which is maximally violated by this realization. Then, one needs to prove that the latter is unique up to the equivalences specified in the definitions above and a possible way to realize this last task is to construct a sum-of-squares decomposition for a given inequality (see, e.g., [21], [23], [72], [74]–[76]) and then solve the resulting algebraic relations for the state and measurements. From the numerical perspective, there are techniques inspired by convex optimization methods, in particular

semi-definite programming (SDP) [25]-[77].

On the other hand, it is worth to comment here that the self-testing schemes have intrinsic limitations. It is known for instance that product states cannot violate Bell inequalities, so there is no way to self-test any product state based on maximal violation of Bell inequalities. Moreover, it is not possible to self-test mixed entangled states from maximal Bell violations because these are always achieved with pure states. It is nevertheless possible to certify some genuinely entangled subspaces (or, equivalently, all mixed states acting on them) [78]. In the case of quantum contextuality it is not possible to certify entangled states because of the "global" unitary freedom involved in the definition of self-testing.

Let us conclude by noting that self-testing might be an interesting option for certification in the device-independent framework (see, e.g., Ref. [18]). In fact, there already exist self-testing schemes for entangled states that are resources for many applications which range from device-independent randomness generation [79], device-independent quantum cryptography [80]–[82], entanglement detection [83], [84] and delegated quantum computing [85], [86]. Also, self-testing can be used to witness the dimension of the underlying quantum system; for instance, in the case of KCBS inequality its maximal violation certifies that the underlying quantum system is at least three-dimensional.

Chapter 2

Paper I

2.1 Sum-of-squares decompositions for a family of noncontextuality inequalities and self-testing of quantum devices

One of the simplest inequalities capable of revealing quantum contextuality is the KCBS inequality, which is a particular case of the n -cycle inequality (1.29) when $n = 5$. In the first article forming the thesis, we consider a modification of the contextuality scenario in which the measurements are not assumed to satisfy any compatibility relations and are performed sequentially on the quantum system, that is, one after the other one. Thus the scenario considered by us pertains to one that is typically referred in the literature to as the temporal scenario (see, e.g., Ref. [87]).

We then derive a novel family of noncontextuality-like inequalities, which are suitable modifications of the n -cycle inequalities, for which one is able to analytically find the corresponding sum-of-squares decompositions. The latter is crucial for determining the maximal quantum violation of the inequalities as well as in deriving the algebraic relations for the state and measurements that enable proving the other main result of our work which is the self-testing result stated in Theorem. It is worth mentioning that the sum-of-squares “technique” has already been used in deriving the maximal quantum values of Bell inequalities as well as in deriving nonlocality-based self-testing statements (see, e.g., Ref. [21]), but has never been used in the contextuality scenario. With the SOS decompositions, we prove that our inequalities can be used for self-testing of three-dimensional quantum state and measurements for the n -cycle scenario for $n = 2^m + 1$ with $m \in \mathbb{N}$.

One of the issues regarding certification schemes based on maximal violation of noncontextuality inequalities is that they require making strong assumptions like that the commutation of measurements and dimension of the Hilbert space [25]. In our work we were able to drop both of them. In fact, our approach is based on a single assumption that requires the measurement device to have no memory and return only the actual post-measurement state. This assumption is certainly much weaker than the assumptions that are considered in the case of the Kochen-Specker contextuality.

Let us finally remark that while the certification methods within the contextuality or sequential measurements scenarios are still not fully device-independent as far as its original definition is concerned, they still allow one to certify systems that do not require spatial separation as in the case of Bell nonlocality. They are also more powerful than the standard quantum tomography since for instance they require performing less measurements and are distinct from those in the prepare-and-measure

scenario because no assumption on the dimensionality of the preparation is required here.

2.2 Author's contribution

My role in this article was:

- Active participation in discussions that lead to designing the main idea of the paper and working out the solution;
- Significant contribution to derivation of the modified KCBS inequalities and in particular the Result 2;
- Analytical derivation of the stabilizing operators presented in Appendix A;
- Help in deriving the main result of the work stated as Theorem;
- Help in preparing the manuscript.

Sum-of-squares decompositions for a family of noncontextuality inequalities and self-testing of quantum devices

Debashis Saha, Rafael Santos, and Remigiusz Augusiak

Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland

Violation of a noncontextuality inequality or the phenomenon referred to ‘quantum contextuality’ is a fundamental feature of quantum theory. In this article, we derive a novel family of noncontextuality inequalities along with their sum-of-squares decompositions in the simplest (odd-cycle) sequential-measurement scenario capable to demonstrate Kochen-Specker contextuality. The sum-of-squares decompositions allow us to obtain the maximal quantum violation of these inequalities and a set of algebraic relations necessarily satisfied by any state and measurements achieving it. With their help, we prove that our inequalities can be used for self-testing of three-dimensional quantum state and measurements. Remarkably, the presented self-testing results rely on a single assumption about the measurement device that is much weaker than the assumptions considered in Kochen-Specker contextuality.

To realize genuine quantum technologies such as cryptographic systems, quantum simulators or quantum computing devices, the back-end user should be ensured that the quantum devices work as specified by the provider. Methods to certify that a quantum device operates in a nonclassical way are therefore needed. The most compelling one, developed in the cryptographic context, is self-testing [MY04]. It exploits nonlocality, i.e., the existence of quantum correlations that cannot be reproduced by the local-realist models, and provides the complete form of device-independent ¹ characterization of quantum devices only from the statistical data the devices generate. Thus, it is being extensively studied in recent years [YVB⁺14, BP15, CGS17].

However, since self-testing, as defined in Ref. [MY04], stands on nonlocality [Bel64] (or, in other words, quantum correlations that violate local-realist inequalities), it is restricted to preparations of composite quantum systems and local measurements on them. Therefore, it poses a fundamental question: presuming the minimum features of the devices how to characterize (i) quantum systems of prime dimension that are not capable of exhibiting nonlocal correlations, and (ii) quantum systems without entanglement or spatial separation between subsystems? A possible way to address such instances is to employ quantum contextuality (Kochen-Specker contextuality), a generalization of nonlocal cor-

relations obtained from the statistics of commuting measurements that are performed on a single quantum system [KS75, Cab08, CSW14, KCBbuS08]. Indeed, the recent study [BRV⁺19b, IMOK20, BRV⁺19a] provides self-testing statements based on contextual correlations (or correlations that violate noncontextuality inequality). Since quantum contextual correlations are essential in many aspects of quantum computation [HWVE14, Rau13] and communication [GHH⁺14, SHP19], self-testing statements are crucial for certifying quantum technology [BRV⁺19a]. Apart from that, it is, nonetheless, fundamentally interesting to seek the maximum information one can infer about the quantum devices only from the observed statistics in a contextuality experiment.

In the context of nonlocality, sum-of-squares (SOS) decomposition of quantum operators associated with local-realist inequalities has been the key mathematical tool in recent years to obtain optimal quantum values and self-testing properties of quantum devices [BP15, ŠASA16, SAT⁺17, KŠT⁺19, SSKA19, ASTA19, Kan19, CMMN19]. Whether this line of study, albeit, restricted to nonlocal correlations, can further be extended to contextuality scenario is of great interest from the perspective of unified approach to non-classical correlations [CSW14, AC18].

In this work, we consider Klyachko-Can-Binicioğlu-Shumovsky (KCBS) scenario which comprises of one preparation and n (where $n \geq 5$ is odd) number of measurements [KCBbuS08, AQB⁺13, LSW11]. This is the simplest scenario capable to exhibit contextual correlations using a three-dimensional quantum system and five binary outcome measurements. It also has several implications in quantum foundation and quantum information [GBC⁺14, GHH⁺14, SBA17, Cab13, KanCK14, SR17, XSS⁺16]. We first introduce a modified version of KCBS expression for $n = 5$ involving correlation between the outcomes of two sequential measurements, along with an SOS decomposition of the respective quantum operator. We describe our methodology to obtain SOS and simultaneously, generalize for n -cycle KCBS scenario where $n = 2^m + 1, m \in \mathbb{N}$. Interestingly, the SOS decomposition holds even without the idealizations that the measurements satisfy commutativity conditions in a cyclic order. By virtue of this decomposition, we obtain the maximum quantum value of our modified n -cycle expression and a set of algebraic relations involving any quantum state and measurements that yield those maximum values. By solving those relations, we show the existence of a three-dimensional vector-space invariant

¹With the requirement of the spatial separation between measurements on subsystems, and without any assumption on the internal features of the devices.

under the algebra of measurement operators. Subsequently, we prove the uniqueness of the projected three-dimensional measurements and state up to unitary equivalence, that is, self-testing property of the quantum devices. The presented self-testing statement relies on the premise that the measurement device returns only the post-measurement system and has no memory, while it does not rely on the commutativity relations between observables.

1 Preliminaries

We begin by illustrating our scenario and specifying the assumptions.

Sequential-measurement set-up. Each run of the experimental observation comprises of preparation of a physical system followed by two measurements in a sequence using one non-demolishing measurement device as depicted in Fig. 1. The measurement device has n (odd) different settings, each of which yields ± 1 outcome. Let's denote the first and second measurement settings by \mathcal{A}_i and \mathcal{A}_j where $i, j \in \{1, \dots, n\}$. The settings are chosen such that $j = i \pm 1$, where from now on the subscript i is taken modulo n , that is, $\mathcal{A}_{i \pm n} = \mathcal{A}_i$. We make the following assumption about the measurement device.

Assumption. *The measurement device has no memory and returns only the actual post-measurement state.*

This assumption is necessary, otherwise, any quantum statistics can be reproduced by classical systems.

By repeating this experiment many times we can obtain joint probabilities $p(a_i, a_{i \pm 1} | \mathcal{A}_i, \mathcal{A}_{i \pm 1})$ of two measurements and single probabilities $p(a_i | \mathcal{A}_i)$ of the first measurement, and consequently, their correlation functions,

$$\begin{aligned} \langle \mathcal{A}_i \mathcal{A}_{i \pm 1} \rangle &= \sum_{a_i, a_{i \pm 1}} a_i a_{i \pm 1} p(a_i, a_{i \pm 1} | \mathcal{A}_i, \mathcal{A}_{i \pm 1}), \\ \langle \mathcal{A}_i \rangle &= \sum_{a_i} a_i p(a_i | \mathcal{A}_i), \end{aligned} \quad (1)$$

where the measurement outcomes are denoted as $a_i = \pm 1$.

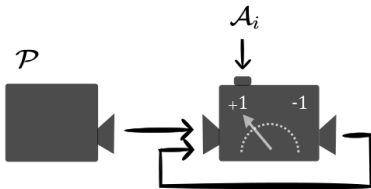


Figure 1: **Sequential-measurement set-up.** The simplest contextuality scenario comprises of one preparation \mathcal{P} and one measurement device with settings \mathcal{A}_i each of them returns ± 1 outcome.

In quantum theory the two-outcome measurements \mathcal{A}_i can be in general non-projective. However, since we do not restrict the dimension of these measurements, an

extension of Naimark's dilation theorem [IMOK20] allows us to consider these measurements to be projective. Thus, we can represent the measurements by the following operators

$$A_i = 2P_i - \mathbb{1}, \quad (2)$$

where P_i are projectors acting on some finite-dimensional Hilbert space \mathcal{H} . The preparation is represented by a quantum state that, by the same reason, can be considered pure; we denote it by $|\psi\rangle$.

Kochen-Specker contextuality [CSW14] pertains to the assumption that the projectors satisfy certain orthogonality relations, particularly in this scenario, $P_i P_{i \pm 1} = 0$ for all i , implying $[A_i, A_{i \pm 1}] = 0$. Such prerequisite about the measurement device are difficult to justify in practice. Since we aim to characterize the quantum devices from their minimal features, we do not make this assumption. We will see later that orthogonality relations between projectors will be derived facts from the maximal violation of our inequality.

A general linear expression that can be considered to test nonclassicality (or noncontextuality in the usual scenario) in this set-up is given by,

$$\mathcal{B} = \sum_i c_i (\langle \mathcal{A}_i \mathcal{A}_{i+1} \rangle + \langle \mathcal{A}_{i+1} \mathcal{A}_i \rangle) + \sum_i d_i \langle \mathcal{A}_i \rangle. \quad (3)$$

Using the quantum expression of the joint probabilities under the aforementioned Assumption, for example, $p(+1, +1 | \mathcal{A}_i, \mathcal{A}_{i \pm 1}) = \langle \psi | P_i P_{i \pm 1} P_i | \psi \rangle$, we find

$$\langle \mathcal{A}_i \mathcal{A}_{i+1} \rangle + \langle \mathcal{A}_{i+1} \mathcal{A}_i \rangle = \langle \psi | \{A_i, A_{i+1}\} | \psi \rangle. \quad (4)$$

Subsequently, the optimal quantum value of the expression (3) is defined as

$$\eta^Q = \sup_{|\psi\rangle, \mathcal{A}_i} \langle \psi | B | \psi \rangle, \quad (5)$$

where $B = \sum_i c_i \{A_i, A_{i+1}\} + \sum_i d_i A_i$ is the quantum operator associated with the expression \mathcal{B} and A_i are of the form (2). Notice that in the usual scenario, due to commutativity relations, $\{A_i, A_{i+1}\}$ can be replaced by $2A_i A_{i+1}$. The maximal classical value η^C (or noncontextual value in the usual scenario ²) is defined as

$$\eta^C = \max_{a_i \in \{1, -1\}} \left\{ 2 \sum_i c_i a_i a_{i+1} + \sum_i d_i a_i \right\}. \quad (6)$$

KCBS inequality. The well known n -cycle KCBS non-contextuality inequality [AQB⁺13] is of the form

$$\mathcal{B}_{\text{KCBS}} := - \sum_{i=1}^n \langle \mathcal{A}_i \mathcal{A}_{i+1} \rangle \leq \eta^C = n - 2. \quad (7)$$

The maximal quantum violation of this inequality is

$$\eta^Q = \frac{3 \cos(\pi/n) - 1}{1 + \cos(\pi/n)} n \quad (8)$$

²Since any noncontextual value assignment pertains to certain orthogonality conditions, here we refer to η^C as the classical value for the relaxed scenario. Note that, under the aforesaid Assumption, the optimal value of \mathcal{B} in classical theory or any other theory where measurement does not affect the system is given by Eq. (6). With the orthogonality conditions, η^C reduces to the maximal non-contextual value.

and it is achieved by the following quantum state

$$|\widehat{\psi}\rangle = |0\rangle \equiv (1, 0, 0)^T, \quad (9)$$

and observables

$$\widehat{A}_i = 2|\widehat{v}_i\rangle\langle\widehat{v}_i| - \mathbb{1}, \quad (10)$$

where $|\widehat{v}_i\rangle$ are three-dimensional real vectors defined as

$$|\widehat{v}_i\rangle = (\cos\theta, \sin\theta \sin\phi_i, \sin\theta \cos\phi_i)^T \quad (11)$$

where θ is defined as $\cos\theta = \sqrt{1/(1+2\alpha)}$, where

$$\alpha = \frac{1}{2} \sec\left(\frac{\pi}{n}\right) \quad (12)$$

and

$$\phi_i = \frac{n-1}{n} \pi i. \quad (13)$$

Note that α and ϕ_i are functions of n , which for the sake of simplification is not explicitly specified in their notation. Let us also remark that $|\widehat{\psi}\rangle \in \mathbb{C}^3$ and \widehat{A}_i acting on \mathbb{C}^3 denote a particular example of quantum realizations achieving the maximal quantum value of the KCBS inequality (7). The self-testing properties of the above-mentioned state and measurements based on the violation of KCBS inequality are shown in [BRV⁺19b]. The proof is based on the optimization method of semidefinite programming under the usual assumptions of contextuality, along with an additional assumption that P_i in Eq. (2) are rank-one projectors.

Sum-of-squares decomposition. Let us finally discuss the concept of sum-of-squares decompositions. Consider a quantum operator B corresponding to some noncontextuality expression \mathcal{B} like the one in (5). Now, if for any choice of quantum measurements A_i and some $\eta \in \mathbb{R}$ one can decompose the shifted operator $\eta\mathbb{1} - B$ as

$$\eta\mathbb{1} - B = \sum_k E_k^\dagger E_k, \quad (14)$$

the maximal quantum value of \mathcal{B} is upper bounded by η , i.e., $\langle\psi|B|\psi\rangle \leq \eta$ for any quantum state $|\psi\rangle$. We call (14) a sum-of-squares decomposition associated to B . Typically E_k are constructed from the measurement operators A_i . The bound η is realized by a state and a set of measurements if and only if the following algebraic relation holds true for all k ,

$$E_k|\psi\rangle = 0. \quad (15)$$

Our self-testing proofs heavily rely on the above relations.

Let us remark that Ref. [LSW11] provides an SOS decomposition for the conventional KCBS operator under the assumptions that the measurements satisfy $[A_i, A_{i\pm 1}] = 0$. In what follows we derive an alternative noncontextuality inequality together with the corresponding SOS decomposition of the form (14) which does not require making this assumption. Furthermore, our SOS is designed in such a way that the algebraic relations (15) it implies can be used for self-testing.

2 Modified KCBS inequality with sum-of-squares decomposition

We are now ready to present our results. For pedagogical purposes we begin with the simplest case of $n = 5$ and consider the following modified KCBS expression

$$\mathcal{B} = -\frac{1}{2} \sum_{i=1}^5 (\langle A_i A_{i+1} \rangle + \langle A_{i+1} A_i \rangle) - \alpha^2 \sum_{i=1}^5 \langle A_i \rangle, \quad (16)$$

where α is given in (12) with $n = 5$. Following (6) it is not difficult to find the maximal classical value of B is $\eta^C = 3 + \alpha^2$.

Result 1 (Modified KCBS inequality with SOS). *The maximal quantum value of \mathcal{B} given in Eq. (16) with $\alpha = (1/2) \sec(\pi/n)$ is $\eta^Q = 3(1 + \alpha^2)$.*

Proof. To prove this statement we present the SOS decomposition for the modified KCBS operator

$$B = -\frac{1}{2} \sum_i \{A_i, A_{i+1}\} - \alpha^2 \sum_i A_i. \quad (17)$$

Let us first define the following Hermitian operators for $i = 1, \dots, 5$,

$$\begin{aligned} M_{i,1} &= -\frac{1}{\alpha^3} (A_i + \alpha A_{i-1} + \alpha A_{i+1}), \\ M_{i,2} &= -\frac{1}{\alpha^4} (-\alpha A_i + A_{i-2} + A_{i+2}), \end{aligned} \quad (18)$$

and observe that they satisfy the following relations

$$-\frac{\alpha^5}{5} \sum_i (2M_{i,1} + \alpha^3 M_{i,2}) = \alpha^2 \sum_i A_i, \quad (19)$$

and

$$\frac{\alpha^5}{5} \sum_i \left(M_{i,1}^2 + \frac{\alpha^3}{2} M_{i,2}^2 \right) = \frac{1}{2} \sum_i \{A_i, A_{i+1}\} + \frac{5}{2\alpha} \mathbb{1}, \quad (20)$$

where we have used the identities $\alpha^2 + \alpha = 1$ for α given in Eq. (12) with $n = 5$ and $A_i^2 = \mathbb{1}$. With the aid of these relations it is straightforward to verify that

$$\begin{aligned} & \frac{\alpha^5}{5} \sum_i (\mathbb{1} - M_{i,1})^2 + \frac{\alpha^8}{10} \sum_i (\mathbb{1} - M_{i,2})^2 \\ &= \left(\alpha^5 + \frac{\alpha^8}{2} \right) \mathbb{1} - \frac{\alpha^5}{5} \sum_i (2M_{i,1} + \alpha^3 M_{i,2}) \\ & \quad + \frac{\alpha^5}{5} \sum_i \left(M_{i,1}^2 + \frac{\alpha^3}{2} M_{i,2}^2 \right) \\ &= 3(1 + \alpha^2) \mathbb{1} - B, \end{aligned} \quad (21)$$

where B is given in Eq. (17).

Thus, the above equation constitutes a SOS decomposition (14) of the modified KCBS operator in which

$$E_k = \sqrt{\frac{\alpha^5}{5}} (\mathbb{1} - M_{k,1}) \quad (22)$$

for $k = 1, \dots, 5$;

$$E_k = \sqrt{\frac{\alpha^8}{10}} (\mathbb{1} - M_{k-5,2}) \quad (23)$$

for $k = 6, \dots, 10$; and $3 + 3\alpha^2 = 4.146$ is the quantum bound of B . We can validate that the state and measurements in dimension three (9)-(10) responsible for optimal value of KCBS inequality achieve this bound. \square

Inspired by the above $n = 5$ case, let us now derive our modified KCBS expression for more measurements. Our aim is to obtain a general expression for which the sum-of-squares decomposition can easily be constructed as the one in Eq. (21) and later directly used for self-testing.

To reach this goal, let us consider n two-outcome quantum measurements represented by operators A_i (2) acting on some Hilbert space of unknown but finite dimension. Let us then consider the expression (14) in which the operators E_k are of the form $\mathbb{1} - M_k$ with some positive multiplicative factors, where M_k are constructed from A_i . Notice that for such a choice, Eq. (15) implies that M_k must be stabilizing operators of the state $|\psi\rangle$ maximally violating our modified KCBS expression, that is, $M_k|\psi\rangle = |\psi\rangle$. Now, to design the explicit form of M_k we can use the optimal quantum realization (9)-(10) of the n -cycle KCBS inequality (7), which gives us (see

Appendix A for details of the derivation)

$$M_{i,k} = \bar{\alpha} [(1 - 2\beta_k) A_i + \beta_k (A_{i+k} + A_{i-k})], \quad (24)$$

where $i = 1, \dots, n$ and $k = 1, \dots, (n-1)/2$, whereas the coefficients β_k and $\bar{\alpha}$ are given by

$$\beta_k = \frac{1}{2(1 - \cos \phi_k)} \quad (25)$$

and

$$\bar{\alpha} = \frac{1 + 2\alpha}{1 - 2\alpha}, \quad (26)$$

where α, ϕ_k are defined in Eqs. (12) and (13), respectively. Let us remark that $M_{i,k}, \bar{\alpha}, \beta_i$ are all functions of n which for the sake of simplification is not specified explicitly. Moreover, the operators $M_{i,k}$ defined in (24) act on unknown Hilbert space \mathcal{H} of finite dimension.

We now go back to the SOS decomposition (14) which is deemed to be of the form

$$\sum_{i,k} c_k [\mathbb{1} - M_{i,k}]^2 \quad (27)$$

with some non-negative parameters c_k to be determined. By plugging the expression of $M_{i,k}$ (24) into it and after some rearrangement of indices, we obtain

$$\begin{aligned} \sum_{i,k} c_k [\mathbb{1} - M_{i,k}]^2 &= \left(n\bar{\alpha}^2 \sum_k c_k \left(\frac{1}{\bar{\alpha}^2} + 1 + 6\beta_k^2 - 4\beta_k \right) \right) \mathbb{1} - \left(2\bar{\alpha} \sum_k c_k \right) \sum_i A_i \\ &\quad + \bar{\alpha}^2 \sum_i \left[2c_1\beta_1 (1 - 2\beta_1) + c_{\frac{n-1}{2}} \beta_{\frac{n-1}{2}}^2 \right] \{A_i, A_{i+1}\} \\ &\quad + \bar{\alpha}^2 \sum_i \sum_{k=2}^{(n-3)/2} \left[2c_k\beta_k (1 - 2\beta_k) + c_{f(\frac{k}{2})} \beta_{f(\frac{k}{2})}^2 \right] \{A_i, A_{i+k}\}, \end{aligned} \quad (28)$$

where

$$f\left(\frac{k}{2}\right) = \begin{cases} k/2, & \text{if } k \text{ is even} \\ (n-k)/2, & \text{if } k \text{ is odd.} \end{cases} \quad (29)$$

We want to choose the coefficient c_k so that they are non-negative and all the anti-commutators $\{A_i, A_{i+k}\}$ vanish except for $k = \pm 1$. For that purpose we consider $n = 2^m + 1$ for $m \in \mathbb{N} \setminus \{1\}$. First we take $c_k = 0$ whenever $k \neq 2^x$, where $x = 0, \dots, m-1$. It follows from (28) that our requirement is fulfilled if the following set of equations is satisfied

$$2c_{2^x}\beta_{2^x}(1 - 2\beta_{2^x}) + c_{2^{x-1}}\beta_{2^{x-1}}^2 = 0 \quad (30)$$

for $x = 1, \dots, m-1$. The above equation (30) implies for all $x = 1, \dots, m-1$

$$\begin{aligned} \frac{c_{2^x}}{c_1} &= \frac{1}{2^x} \prod_{j=1}^x \frac{\beta_{2^{j-1}}^2}{\beta_{2^j}(2\beta_{2^j} - 1)} \\ &= \left(\frac{\beta_1}{2^x\beta_{2^x}} \right)^2 \prod_{j=1}^x \sec(\phi_{2^j}). \end{aligned} \quad (31)$$

Since $\sec(\phi_{2^j})$ is positive for all j ³, c_{2^x}/c_1 is also positive. Now, to provide a plausible solution of c_{2^x} , it suffices to choose a positive c_1 . Due to (30) the remaining anti-commutators in (28) are $\{A_i, A_{i+1}\}$ with a factor

$$\bar{\alpha}^2 [2c_1\beta_1(1 - 2\beta_1) + c_{2^{m-1}}\beta_{2^{m-1}}^2]. \quad (32)$$

For simplicity we choose this factor to be 1/2 which implies that c_1 is such that

$$4c_1\beta_1(1 - 2\beta_1) + 2c_{2^{m-1}}\beta_{2^{m-1}}^2 = \frac{1}{\bar{\alpha}^2}. \quad (33)$$

After substituting $c_{2^{m-1}}$ from Eq. (31), the above gives

$$c_1 = \frac{2^{2m-3}}{\bar{\alpha}^2} \frac{1}{2^{2m-1}\beta_1(1 - 2\beta_1) + \beta_1^2 \prod_{j=1}^{m-1} \sec(\phi_{2^j})}. \quad (34)$$

One can readily verify that c_1 is positive. Finally, due to

³Note that $\cos \phi_{2^j} = \cos(\pi 2^j/n)$ and $0 < \pi 2^j/n < \pi/2, \forall j = 1, 2, \dots, m-1$.

(30) and (33), Eq. (28) reads as,

$$\sum_{i,k} c_k [\mathbb{1} - M_{i,k}]^2 = \eta_n \mathbb{1} - B_n, \quad (35)$$

where

$$B_n = -\frac{1}{2} \sum_i \{A_i, A_{i+1}\} - \gamma \sum_i A_i, \quad (36)$$

$$\gamma = -2\bar{\alpha} \sum_k c_k, \quad (37)$$

and

$$\eta_n = n\bar{\alpha}^2 \sum_k c_k \left(\frac{1}{\bar{\alpha}^2} + 1 + 6\beta_k^2 - 4\beta_k \right), \quad (38)$$

and $c_k, M_{i,k}$ are defined in (31), (34) and (24).

From Eq. (25) we know that $\bar{\alpha}$ is a negative quantity and hence γ is positive. Thus, our modified n -cycle KCBS inequality is

$$\mathcal{B}_n := -\frac{1}{2} \sum_i (\langle A_i A_{i+1} \rangle + \langle A_{i+1} A_i \rangle) - \gamma \sum_i \langle A_i \rangle \leq \eta_n^C \quad (39)$$

whose quantum bound is η_n (38) and the classical value η_n^C is provided in *Result 3*. It follows from the construction of the SOS (35) that the qutrit quantum state and measurements defined in Eqs. (9)-(13) satisfy the stabilizing relations $M_{i,k}|\psi\rangle = |\psi\rangle$, implying the bound η_n is tight, or, in other words, the maximal quantum value of (39) equals η_n .

To put the above mathematical analysis in a nutshell, the expression of the noncontextuality inequality (39) is derived such that it meets a SOS decomposition (14) of certain form. This leads us to the following result.

Result 2 (Modified n -cycle expression with SOS). *The maximum quantum value of modified n -cycle noncontextuality expression (39) with a SOS decomposition (35) is η_n (38) (where $n = 2^m + 1, m \in \mathbb{N} \setminus \{1\}$).*

Let us finally prove the classical bound of our new non-contextuality expression.

Result 3 (Maximal classical value). *The classical value of \mathcal{B}_n in Eq. (39) is given by $n + \gamma - 2$.*

Proof. The classical value can be obtained by assigning ± 1 values to the observables appearing in (39), that is,

$$\eta_n^C = \max_{a_i \in \{1, -1\}} \left\{ -\sum_{i=1}^n a_i a_{i+1} - \gamma \sum_{i=1}^n a_i \right\}, \quad (40)$$

where γ is positive. Let us say in the optimal assignment there are k number of a_i which are -1 . We first assume $k > n/2$. When there are k number of -1 , and $n - k$ number of $+1$, the minimum value of $\sum_i a_i a_{i+1} = 4k - 3n$, and the quantity $\sum_i a_i = n - 2k$. Substituting these values in (40) we see

$$\eta_n^C = (3 - \gamma)n - (4 - 2\gamma)k. \quad (41)$$

Therefore, the optimal value of η_n^C is obtained for the minimum value of k , that is, for $k = (n + 1)/2$. This implies the right-hand-side of (41) is $n + \gamma - 2$. Similarly, if $k < n/2$, then we have $(n - k) > n/2$, and following a similar argument we can obtain the same bound. \square

3 Self-testing of quantum devices

An exact self-testing statement provides us the certification of quantum devices, given that we observe an optimal violation of a noncontextuality inequality. However, the observed statistics are unchanged in the presence of auxiliary degrees of freedom (or auxiliary systems) and a global unitary. Therefore, self-testing in the context of state-dependent quantum contextual correlation [BRV⁺19b, IMOK20] infers unique state and measurements up to these equivalences.

Here, we take the definition of self-testing stated in [IMOK20]. Formally, self-testing of preparation $|\bar{\psi}\rangle \in \mathbb{C}^d$ and a set of measurements $\{\bar{A}_i\}_{i=1}^n$ acting on \mathbb{C}^d is defined as follows: if a set of observables $\{A_i\}_{i=1}^n$ acting on unknown finite-dimensional Hilbert space \mathcal{H} and a state $|\psi\rangle \in \mathcal{H}$ maximally violate a noncontextuality inequality, then there exists a projection $\mathbb{P} : \mathcal{H} \rightarrow \mathbb{C}^d$ and a unitary operation U on \mathbb{C}^d such that

1. $U(\mathbb{P}|\psi\rangle) = |\bar{\psi}\rangle$,
2. $U(\mathbb{P}A_i\mathbb{P})U^\dagger = \bar{A}_i$ for all $i = 1, \dots, n$.

To obtain self-testing only from the reduced Assumption mentioned in section 1, we consider a modified version of the expression \mathcal{B}_n (39) of the following form

$$\tilde{\mathcal{B}}_n := \mathcal{B}_n - \sum_i [p(++|A_{i+1}, A_i) + p(++|A_{i-1}, A_i)]. \quad (42)$$

Since the additional term is non-positive, the classical and quantum bounds of $\tilde{\mathcal{B}}_n$ are the same as for \mathcal{B}_n . Moreover, it follows from (35) that the SOS decomposition of $\tilde{\mathcal{B}}_n$ is

$$\begin{aligned} \eta_n \mathbb{1} - \tilde{\mathcal{B}}_n &= \sum_{i,k} c_k [\mathbb{1} - M_{i,k}]^2 + \sum_i (P_i P_{i+1})^\dagger (P_i P_{i+1}) \\ &\quad + \sum_i (P_i P_{i-1})^\dagger (P_i P_{i-1}), \end{aligned} \quad (43)$$

where

$$\tilde{\mathcal{B}}_n = \mathcal{B}_n - \sum_i P_{i+1} P_i P_{i+1} - \sum_i P_{i-1} P_i P_{i-1}, \quad (44)$$

and η_n is again the optimal quantum value of $\tilde{\mathcal{B}}_n$. Let us now show that our inequality (42) can be used to make a self-testing statement, according to the above definition, for the state and observables (9)-(10) maximally violating it.

Result 4 (Self-testing). *Under the Assumption stated in Sec. 1, if a quantum state $|\psi\rangle \in \mathcal{H}$ and a set of n (where $n = 2^m + 1, m \in \mathbb{N} \setminus \{1\}$) measurements A_i acting on \mathcal{H} violate the inequality (42) maximally, then there exists a projection $\mathbb{P} : \mathcal{H} \rightarrow \mathbb{C}^3$ and a unitary U acting on \mathbb{C}^3 such that*

$$\begin{aligned} U(\mathbb{P}A_i\mathbb{P}^\dagger)U^\dagger &= 2|\hat{v}_i\rangle\langle\hat{v}_i| - \mathbb{1}_3, \\ U(\mathbb{P}|\psi\rangle) &= (1, 0, 0)^T, \end{aligned} \quad (45)$$

where $|\hat{v}_i\rangle$ are defined in (11).

Proof. Taking the expectation value of the state $|\psi\rangle$ on both side of the SOS decomposition (43) of \mathcal{B} , we obtain by virtue of (15) that for any i and k ,

$$M_{i,k}|\psi\rangle = |\psi\rangle. \quad (46)$$

In the particular $k = 1$ case this condition when combined with the explicit form of $M_{i,1}$ given in Eq. (24) together with the fact that $\beta_1 = \alpha/(1+2\alpha)$, leads to the following relations for all $i = 1, \dots, n$,

$$(A_i + \alpha A_{i+1} + \alpha A_{i-1})|\psi\rangle = (1 - 2\alpha)|\psi\rangle. \quad (47)$$

Similarly, from the last two terms of the SOS decomposition (43) we get that for all $i = 1, \dots, n$,

$$P_i P_{i\pm 1}|\psi\rangle = 0. \quad (48)$$

Given the relations (47) and (48), the next Theorem provides the proof for the self-testing statement. \square

The self-testing property implies our modified inequality (42) are non-trivial since any classical value assignment is not equivalent to the realization given in (45).

Theorem. *If a set of quantum observables $\{A_i\}_{i=1}^n$ (where n is odd) of the form (2) acting on arbitrary finite-dimensional Hilbert space \mathcal{H} and a unit vector $|\psi\rangle \in \mathcal{H}$ satisfy the relations (47) and (48), then there exists a projection operator $\mathbb{P} : \mathcal{H} \rightarrow \mathbb{C}^3$ and a unitary U acting on \mathbb{C}^3 such that (45) holds true.*

Proof. We prove this theorem in two steps.

Step 1. In the first step, we deduce the effective dimensionality of the observables A_i and the state $|\psi\rangle$. Let us define a vector space $V = \text{Span}\{|\psi\rangle, A_1|\psi\rangle, A_3|\psi\rangle\}$. Due to Lemma 1 (stated in Appendix B), it suffices to consider the observables A_i and the state $|\psi\rangle$ restricted to V . In other words, Lemma 1 points out that the Hilbert space \mathcal{H} can be decomposed as $V \oplus V^\perp$ and all the operators A_i have the following block structure

$$A_i = \begin{pmatrix} \tilde{A}_i & \mathbb{O} \\ \mathbb{O} & A'_i \end{pmatrix}, \quad (49)$$

wherein \tilde{A}_i, A'_i are acting on V, V^\perp , respectively; in particular, $A'_i|\psi\rangle = 0$ for any i . This allows us to define

$$\begin{aligned} \tilde{A}_i &= \mathbb{P} A_i \mathbb{P}^\dagger = 2\tilde{P}_i - \mathbb{1}, \\ |\tilde{\psi}\rangle &= \mathbb{P}|\psi\rangle, \end{aligned} \quad (50)$$

where \mathbb{P} is the projection operator from \mathcal{H} to V , $\tilde{P}_i = \mathbb{P} P_i \mathbb{P}^\dagger \geq 0$ and $\mathbb{1}$ is the identity operator acting on V .

It follows from Eq. (2) and Eqs. (47) and (48) that the projected measurements \tilde{P}_i and the state $|\tilde{\psi}\rangle$ satisfy the following sets of relations for all $i = 1, \dots, n$,

$$\tilde{P}_i \tilde{P}_{i\pm 1} |\tilde{\psi}\rangle = 0, \quad (51)$$

$$(\tilde{P}_i + \alpha \tilde{P}_{i-1} + \alpha \tilde{P}_{i+1}) |\tilde{\psi}\rangle = |\tilde{\psi}\rangle, \quad (52)$$

Step 2. In the second step, we characterize the observables \tilde{A}_i . With the help of Lemma 2 given in Appendix B, we first show that all observables \tilde{A}_i are of the form

$$\tilde{A}_i = 2|v_i\rangle\langle v_i| - \mathbb{1} \quad (53)$$

for some normalized vectors $|v_i\rangle \in \mathbb{C}^3$ such that $\langle v_i | v_{i\pm 1} \rangle = 0$. The remaining part is the characterization of $|v_i\rangle$. By plugging Eq. (53) into Eq. (52) we obtain that for all i ,

$$(|v_i\rangle\langle v_i| + \alpha |v_{i-1}\rangle\langle v_{i-1}| + \alpha |v_{i+1}\rangle\langle v_{i+1}|)|\tilde{\psi}\rangle = |\tilde{\psi}\rangle. \quad (54)$$

We use the fact that $|v_i\rangle, |v_{i\pm 1}\rangle$ are orthogonal and multiply $\langle v_{i-1}|$ and $\langle v_{i+1}|$ with Eq. (54), which lead us to the following equations

$$\alpha \langle v_{i-1} | v_{i+1} \rangle \langle v_{i+1} | \tilde{\psi} \rangle = (1 - \alpha) \langle v_{i-1} | \tilde{\psi} \rangle \quad (55)$$

and

$$\alpha \langle v_{i+1} | v_{i-1} \rangle \langle v_{i-1} | \tilde{\psi} \rangle = (1 - \alpha) \langle v_{i+1} | \tilde{\psi} \rangle \quad (56)$$

for all i . By substituting the term $\langle v_{i-1} | \tilde{\psi} \rangle$ from the first equation to the second one, we arrive at the following conditions

$$\forall i, \quad |\langle v_{i-1} | v_{i+1} \rangle| = \frac{1 - \alpha}{\alpha}. \quad (57)$$

Note that, here we use the fact that $\langle v_{i+1} | \tilde{\psi} \rangle \neq 0$ ⁴. Considering the absolute value of both side of (56) and using (57) we obtain another set of conditions

$$\forall i, \quad |\langle \tilde{\psi} | v_{i-1} \rangle| = |\langle \tilde{\psi} | v_{i+1} \rangle|. \quad (58)$$

And since n is odd, as a consequence of the above equation,

$$\forall i, j, \quad |\langle \tilde{\psi} | v_i \rangle| = |\langle \tilde{\psi} | v_j \rangle|. \quad (59)$$

Let us try to see what is the most general form of $|v_i\rangle$ compatible with the above conditions. First let us exploit the fact that observed probabilities do not change if we rotate the state and measurements by a unitary operation. We thus choose it so that $U|\tilde{\psi}\rangle = (1, 0, 0)^T \equiv |0\rangle$. We also notice that any unitary of the following form

$$\begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix} \quad (60)$$

with U' being any 2×2 unitary does not change $|0\rangle$. Later we will use this freedom.

Due to the fact that we are characterizing projectors $|v_i\rangle\langle v_i|$ rather than the vectors themselves, we can always assume the first element of the vector is positive, that is, $|v_i\rangle$ has the form,

$$|v_i\rangle = (\cos \theta_i, e^{ia_i} \sin \theta_i \sin \phi_i, e^{ib_i} \sin \theta_i \cos \phi_i)^T. \quad (61)$$

The condition (59) implies that all $\cos \theta_i$ are equal and therefore let us denote $\theta_i = \theta$. Plugging these forms of $|v_i\rangle$ and $|\tilde{\psi}\rangle = |0\rangle$ into Eq. (54), the first element of the vector equation leads to

$$\cos \theta = \frac{1}{\sqrt{1 + 2\alpha}}. \quad (62)$$

⁴If $\langle v_{j+1} | \tilde{\psi} \rangle = 0$ for some j , then (55) implies $\langle v_{j-1} | \tilde{\psi} \rangle$ is also 0, and further (54) implies $|v_j\rangle\langle v_j | \tilde{\psi} \rangle = |\tilde{\psi}\rangle$. Substituting these in (54) taking $i = j + 1$, we arrive at a relation $|v_{j+2}\rangle\langle v_{j+2} | \tilde{\psi} \rangle = (1 - \alpha)/\alpha |\tilde{\psi}\rangle$ which cannot be true for any finite n since $|v_{j+2}\rangle\langle v_{j+2} |$ has eigenvalues 1,0.

Using this freedom we can bring one of the vectors, say $|v_n\rangle$, to $(\cos \theta, 0, \sin \theta)^T$ by taking

$$\sin \phi_n = 0, \quad e^{ib_n} = 1. \quad (63)$$

Then, due to the condition $\langle v_1 | v_n \rangle = \langle v_{n-1} | v_n \rangle = 0$ we infer $e^{ib_1}, e^{ib_{n-1}}$ are real and without loss of generality we can take

$$e^{ib_1} = e^{ib_{n-1}} = 1 \quad (64)$$

by absorbing the sign in $\cos \phi_1, \cos \phi_{n-1}$. Further, we can get rid one of the phases in $|v_1\rangle$, that is,

$$e^{ia_1} = 1, \quad (65)$$

and take $\sin(\phi_1)$ to be non-negative by applying another unitary of the form (60),

$$U' = \text{diag}[\pm \exp(-ia_1), 1] \quad (66)$$

that does not change the simplified form of $|v_n\rangle$. Equating the second and third element of the vector equation (54), we obtain the relations

$$e^{ia_i} \sin \phi_i + \alpha e^{ia_{i-1}} \sin \phi_{i-1} + \alpha e^{ia_{i+1}} \sin \phi_{i+1} = 0, \quad (67)$$

and

$$e^{ib_i} \cos \phi_i + \alpha e^{ib_{i-1}} \cos \phi_{i-1} + \alpha e^{ib_{i+1}} \cos \phi_{i+1} = 0. \quad (68)$$

With the aid of (63) and (65), Eq. (67) for $i = n$ points out $\sin(\phi_1) = -e^{ia_{n-1}} \sin(\phi_{n-1})$ which allows us to consider $e^{ia_{n-1}} = 1$. Taking $i = 1$ in Eqs. (67) and (68) and replacing the values of $\sin \phi_n, \cos \phi_n, e^{ia_1}, e^{ib_1}, e^{ib_n}$ we obtain,

$$\sin \phi_1 + \alpha e^{ia_2} \sin \phi_2 = 0, \quad (69)$$

$$\cos \phi_1 + \alpha + \alpha e^{ib_2} \cos \phi_2 = 0. \quad (70)$$

Thus, e^{ia_2}, e^{ib_2} are real and can be taken to be 1. Note, here we use the fact that $\sin \phi_1 \neq 0$ ⁵. Similarly, by taking $i = 2, \dots, n-2$ we conclude for all i

$$e^{ia_i} = e^{ib_i} = 1. \quad (71)$$

On the other hand, the condition $\langle v_i | v_{i+1} \rangle = 0$ implies,

$$\begin{aligned} \phi_{i+1} - \phi_i &= \cos^{-1} \left(-\frac{\cos^2 \theta}{\sin^2 \theta} \right) \\ &= \frac{(n-1)\pi}{n}. \end{aligned} \quad (72)$$

Finally, considering $i = n$ in the above Eq. (72) and using $\sin \phi_n = 0$ we deduce $\phi_1 = (n-1)\pi/n$. We discard the possibility $\phi_1 = -(n-1)\pi/n$ since $\sin \phi_1$ is taken to be non-negative. Thus, the equations (62), (71), and (72) together with ϕ_1 establish that the unknown vectors $|v_i\rangle$ in (61) are unitarily equivalent to $|\hat{v}_i\rangle$. This completes the proof. \square

⁵If $\sin \phi_1 = 0$, then $\cos \phi_1 = \pm 1$ and consequently $\langle v_n | v_1 \rangle = \cos(\theta \mp \theta)$ which contradicts the relation $\langle v_n | v_1 \rangle = 0$. Analogously, if we suppose $\cos \phi_2 = 0$, then $\cos \phi_1 + \alpha = 0$ and $\sin \phi_2 = \pm 1$. Now, the first equation holds only if $2\alpha^2 = 1$.

4 Conclusion

Kochen-Specker contextuality captures the intrinsic nature of quantum theory that essentially departs from classicality. It also offers a generalization of quantum correlations beyond nonlocality to a larger class of quantum systems and minimizes the demands to test non-classicality. Therefore, it is a fundamental problem to understand what is the maximal information about the underlying quantum system that can be inferred from the correlations observed in a contextuality experiment, and whether this information can be used for certification of quantum devices from minimal assumptions of their internal functioning.

In this work, we derive self-testing statements for n -cycle scenario using weaker assumptions than those made in previous approaches based on Kochen-Specker contextuality [CSW14, BRV⁺19b, IMOK20, BRV⁺19a]. In particular, we do not assume orthogonality relations between measurement effects. Instead, we consider general two-outcome measurements which nevertheless obey a single assumption that the measurement device does not return any additional information except the post-measurement system and does not possess any memory. Moreover, we take a different approach, that is, we use the sum-of-squares 'technique' that has successfully been used in the Bell scenario to derive maximal quantum violation of certain Bell inequalities as well as in making self-testing statements [BP15, ŠASA16, SAT⁺17, KŠT⁺19, SSKA19, CMMN19, Kan19, ASTA19], but has never been explored for self-testing in the contextuality scenario.

We further remark that self-testing from quantum contextuality is not fully device-independent as far as its original definition is concerned, while, its experimental test does not require space-like separation. The assumption is critical to verify for practical purposes, however, in future studies, one may try to overcome it by restricting the computational power or the memory of the measurement device. Nonetheless, it is way more powerful than the usual process of tomography. It is also distinct from the self-testing approach in prepare-and-measure scenario [TKV⁺18, FK19] since no restriction on the dimensionality of the preparation is imposed here.

Although the SOS decompositions hold for a certain number of measurements, a suitable adaptation of our approach in future studies may lead to SOS decompositions for an arbitrary odd number of measurements. Another direction for further study is to explore whether our approach can be applied to states and measurements of higher dimension than three and whether our self-testing statements can be made robust to experimental imperfections. From a more general perspective, it would be interesting to design a unifying approach to self-testing based on Bell nonlocality and quantum contextuality.

Acknowledgement

This work is supported by the Foundation for Polish Science through the First Team project (First TEAM/2017-4/31) co-financed by the European Union under the Eu-

References

- [AC18] B. Amaral and M. T. Cunha. *Contextuality: The Compatibility-Hypergraph Approach*, pages 13–48. Springer Briefs in Mathematics. Springer, Cham, 2018. DOI: [10.1007/978-3-319-93827-1_2](https://doi.org/10.1007/978-3-319-93827-1_2).
- [AQB⁺13] M. Araújo, M. T. Quintino, C. Budroni, M. T. Cunha, and A. Cabello. All noncontextuality inequalities for the n -cycle scenario. *Phys. Rev. A*, 88: 022118, 2013. DOI: [10.1103/PhysRevA.88.022118](https://doi.org/10.1103/PhysRevA.88.022118).
- [ASTA19] R. Augusiak, A. Salavrakos, J. Tura, and A. Acín. Bell inequalities tailored to the Greenberger–Horne–Zeilinger states of arbitrary local dimension. *New J. Phys.*, 21(11): 113001, 2019. DOI: [10.1088/1367-2630/ab4d9f](https://doi.org/10.1088/1367-2630/ab4d9f).
- [Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1: 195–200, 1964. DOI: [10.1103/PhysicsPhysiqueFizika.1.195](https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195).
- [BP15] C. Bamps and S. Pironio. Sum-of-squares decompositions for a family of Clauser–Horne–Shimony–Holt-like inequalities and their application to self-testing. *Phys. Rev. A*, 91: 052111, 2015. DOI: [10.1103/PhysRevA.91.052111](https://doi.org/10.1103/PhysRevA.91.052111).
- [BRV⁺19a] K. Bharti, M. Ray, A. Varvitsiotis, A. Cabello, and L. Kwek. Local certification of programmable quantum devices of arbitrary high dimensionality. 2019.
- [BRV⁺19b] K. Bharti, M. Ray, A. Varvitsiotis, N. Warsi, A. Cabello, and L. Kwek. Robust Self-Testing of Quantum Systems via Noncontextuality Inequalities. *Phys. Rev. Lett.*, 122: 250403, 2019. DOI: [10.1103/PhysRevLett.122.250403](https://doi.org/10.1103/PhysRevLett.122.250403).
- [Cab08] A. Cabello. Experimentally Testable State-Independent Quantum Contextuality. *Phys. Rev. Lett.*, 101: 210401, 2008. DOI: [10.1103/PhysRevLett.101.210401](https://doi.org/10.1103/PhysRevLett.101.210401).
- [Cab13] A. Cabello. Simple Explanation of the Quantum Violation of a Fundamental Inequality. *Phys. Rev. Lett.*, 110: 060402, 2013. DOI: [10.1103/PhysRevLett.110.060402](https://doi.org/10.1103/PhysRevLett.110.060402).
- [CGS17] A. Coladangelo, K. Goh, and V. Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8(1): 15485, 2017. DOI: [10.1038/ncomms15485](https://doi.org/10.1038/ncomms15485).
- [CMMN19] D. Cui, A. Mehta, H. Mousavi, and S. Nezhadi. A generalization of CHSH and the algebraic structure of optimal strategies. 2019.
- [CSW14] A. Cabello, S. Severini, and A. Winter. Graph-Theoretic Approach to Quantum Correlations. *Phys. Rev. Lett.*, 112: 040401, 2014. DOI: [10.1103/PhysRevLett.112.040401](https://doi.org/10.1103/PhysRevLett.112.040401).
- [FK19] M. Farkas and J. Kaniewski. Self-testing mutually unbiased bases in the prepare-and-measure scenario. *Phys. Rev. A*, 99: 032316, 2019. DOI: [10.1103/PhysRevA.99.032316](https://doi.org/10.1103/PhysRevA.99.032316).
- [GBC⁺14] O. Gühne, C. Budroni, A. Cabello, M. Kleinmann, and J. Larsson. Bounding the quantum dimension with contextuality. *Phys. Rev. A*, 89: 062107, 2014. DOI: [10.1103/PhysRevA.89.062107](https://doi.org/10.1103/PhysRevA.89.062107).
- [GHH⁺14] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, and A. Wójcik. Quantifying Contextuality. *Phys. Rev. Lett.*, 112: 120401, 2014. DOI: [10.1103/PhysRevLett.112.120401](https://doi.org/10.1103/PhysRevLett.112.120401).
- [HWVE14] M. Howard, J. Wallman, V. Veitch, and J. Emerson. Contextuality supplies the “magic” for quantum computation. *Nature*, 510(7505): 351–355, 2014. DOI: [10.1038/nature13460](https://doi.org/10.1038/nature13460).
- [IMOK20] A. Irfan, K. Mayer, G. Ortiz, and E. Knill. Certified quantum measurement of Majorana fermions. *Phys. Rev. A*, 101: 032106, 2020. DOI: [10.1103/PhysRevA.101.032106](https://doi.org/10.1103/PhysRevA.101.032106).
- [Kan19] J. Kaniewski. A weak form of self-testing. 2019.
- [KanCK14] P. Kurzyński, A. Cabello, and D. Kaszlikowski. Fundamental Monogamy Relation between Contextuality and Nonlocality. *Phys. Rev. Lett.*, 112: 100401, 2014. DOI: [10.1103/PhysRevLett.112.100401](https://doi.org/10.1103/PhysRevLett.112.100401).
- [KCBbuS08] A. Klyachko, M. Can, S. Binicioğlu, and A. Shumovsky. Simple Test for Hidden Variables in Spin-1 Systems. *Phys. Rev. Lett.*, 101: 020403, 2008. DOI: [10.1103/PhysRevLett.101.020403](https://doi.org/10.1103/PhysRevLett.101.020403).
- [KS75] S. Kochen and E. Specker. The Problem of Hidden Variables in Quantum Mechanics. In *The Logico-Algebraic Approach to Quantum Mechanics*, The Western Ontario Series in Philosophy of Science, pages 293–328. Springer Netherlands, 1975. DOI: [10.1007/978-94-010-1795-4](https://doi.org/10.1007/978-94-010-1795-4).
- [KŠT⁺19] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems.

- Quantum*, 3: 198, 2019.
DOI: [10.22331/q-2019-10-24-198](https://doi.org/10.22331/q-2019-10-24-198).
- [LSW11] Y. Liang, R. Spekkens, and H. Wiseman. Specker’s parable of the overprotective seer: A road to contextuality, nonlocality and complementarity. *Phys. Rep.*, 506(1): 1–39, 2011.
DOI: [10.1016/j.physrep.2011.05.001](https://doi.org/10.1016/j.physrep.2011.05.001).
- [MY04] D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Inf. Comput.*, 4(4): 273–286, 2004.
DOI: doi.org/10.26421/QIC4.4.
- [Rau13] R. Raussendorf. Contextuality in measurement-based quantum computation. *Phys. Rev. A*, 88: 022322, 2013.
DOI: [10.1103/PhysRevA.88.022322](https://doi.org/10.1103/PhysRevA.88.022322).
- [ŠASA16] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín. Self-testing protocols based on the chained bell inequalities. *New J. Phys.*, 18(3): 035013, 2016.
DOI: [10.1088/1367-2630/18/3/035013](https://doi.org/10.1088/1367-2630/18/3/035013).
- [SAT⁺17] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio. Bell Inequalities Tailored to Maximally Entangled States. *Phys. Rev. Lett.*, 119: 040402, 2017.
DOI: [10.1103/PhysRevLett.119.040402](https://doi.org/10.1103/PhysRevLett.119.040402).
- [SBA17] J. Singh, K. Bharti, and Arvind. Quantum key distribution protocol based on contextuality monogamy. *Phys. Rev. A*, 95: 062333, 2017.
DOI: [10.1103/PhysRevA.95.062333](https://doi.org/10.1103/PhysRevA.95.062333).
- [SHP19] D. Saha, P. Horodecki, and M. Pawłowski. State independent contextuality advances one-way communication. *New J. Phys.*, 21(9): 093057, 2019.
DOI: [10.1088/1367-2630/ab4149](https://doi.org/10.1088/1367-2630/ab4149).
- [SR17] D. Saha and R. Ramanathan. Activation of monogamy in nonlocality using local contextuality. *Phys. Rev. A*, 95: 030104, 2017.
DOI: [10.1103/PhysRevA.95.030104](https://doi.org/10.1103/PhysRevA.95.030104).
- [SSKA19] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak. Self-testing quantum systems of arbitrary local dimension with minimal number of measurements. 2019.
- [TKV⁺18] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner. Self-testing quantum states and measurements in the prepare-and-measure scenario. *Phys. Rev. A*, 98: 062307, 2018.
DOI: [10.1103/PhysRevA.98.062307](https://doi.org/10.1103/PhysRevA.98.062307).
- [XSS⁺16] Z. Xu, D. Saha, H. Su, M. Pawłowski, and J. Chen. Reformulating noncontextuality inequalities in an operational approach. *Phys. Rev. A*, 94: 062103, 2016.
DOI: [10.1103/PhysRevA.94.062103](https://doi.org/10.1103/PhysRevA.94.062103).
- [YVB⁺14] T. Yang, T. Vértesi, J. Bancal, V. Scarani, and M. Navascués. Robust and Versatile Black-Box Certification of Quantum Devices. *Phys. Rev. Lett.*, 113: 040401, 2014.
DOI: [10.1103/PhysRevLett.113.040401](https://doi.org/10.1103/PhysRevLett.113.040401).

A Obtaining the stabilizing operators

To guess the stabilizing operators $M_{i,k}$ we use the stabilizing operators in the optimal quantum realization of n -cycle KCBS inequality (7). Let us assume that these operators are in the following form

$$\widehat{M}_{i,k} = a\widehat{A}_i + b\widehat{A}_{i+k} + b'\widehat{A}_{i-k}, \quad (73)$$

where the coefficients a , b and b' are to be determined as a solution to the equation

$$(a\widehat{A}_i + b\widehat{A}_{i+k} + b'\widehat{A}_{i-k})|\widehat{\psi}\rangle = |\widehat{\psi}\rangle, \quad (74)$$

and $|\widehat{\psi}\rangle, \widehat{A}_i$ are given in Eqs. (9)-(10). To solve the above we first notice the following relation,

$$\widehat{A}_i|\widehat{\psi}\rangle = (\cos 2\theta, \sin 2\theta \sin \phi_i, \sin 2\theta \cos \phi_i)^T, \quad (75)$$

which when substituted into Eq. (74) leads one to a system of equations

$$\begin{bmatrix} a(1 + \frac{b}{a} + \frac{b'}{a}) \cos 2\theta \\ a \sin 2\theta (\sin \phi_i + \frac{b}{a} \sin \phi_{i+k} + \frac{b'}{a} \sin \phi_{i-k}) \\ a \sin 2\theta (\cos \phi_i + \frac{b}{a} \cos \phi_{i+k} + \frac{b'}{a} \cos \phi_{i-k}) \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}. \quad (76)$$

Assuming that $a \neq 0$ and taking into account that $\sin 2\theta \neq 0$, the last two equations in the above system can be rewritten as

$$\begin{bmatrix} \sin \phi_i & \sin \phi_{i+k} & \sin \phi_{i-k} \\ \cos \phi_i & \cos \phi_{i+k} & \cos \phi_{i-k} \end{bmatrix} \begin{bmatrix} 1 \\ b/a \\ b'/a \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \quad (77)$$

After multiplying the above equation from left by

$$\begin{bmatrix} \sin \phi_i & \cos \phi_i \\ \cos \phi_i & -\sin \phi_i \end{bmatrix} \quad (78)$$

and using the fact $\phi_{i+k} - \phi_i = \phi_k$, Eq. (77) simplifies to,

$$\begin{bmatrix} 1 & \cos \phi_k & \cos \phi_k \\ 0 & \sin \phi_k & -\sin \phi_k \end{bmatrix} \begin{bmatrix} 1 \\ b/a \\ b'/a \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \quad (79)$$

In this way we remark that the dependence of i in (77) disappears and the system of equations (79) imply

$$\frac{b}{a} = \frac{b'}{a} = -\frac{1}{2} \sec \phi_k. \quad (80)$$

Substitution of above in the first vector equality of (76) leads to

$$a = \frac{1}{(1 - \sec \phi_k)(2 \cos^2 \theta - 1)}, \quad (81)$$

and thus, we obtain a unique solution of a, b, b' . Finally, substituting a, b, b' into Eq. (74) we can conveniently state $\widehat{M}_{i,k}$ operators in the following way

$$\widehat{M}_{i,k} := \left(\frac{1+2\alpha}{1-2\alpha} \right) \left[(1-2\beta_k)\widehat{A}_i + \beta_k(\widehat{A}_{i+k} + \widehat{A}_{i-k}) \right], \quad (82)$$

where

$$\beta_k = \frac{1}{2(1 - \cos \phi_k)}, \quad \alpha = \frac{1}{2} \sec \left(\frac{\pi}{n} \right). \quad (83)$$

B Lemma 1-2

In this appendix, we provide two Lemmas that are used in the proof of the Theorem.

Lemma 1. *If a set of quantum observables $\{A_i\}_{i=1}^n$ (where n is odd) of the form (2) and a vector $|\psi\rangle$ satisfy the relations (47) and (48), then the vector space*

$$V = \text{span}\{|\psi\rangle, A_1|\psi\rangle, A_3|\psi\rangle\} \quad (84)$$

is invariant under the algebra generated by A_i .

Proof. To prove this statement it suffices to show that $A_i|\psi\rangle$ for all $i = 1, \dots, n$ as well as all $A_i A_j|\psi\rangle$ with $i \neq j$ can be expressed as linear combinations of the basis vectors $|\psi\rangle, A_1|\psi\rangle$ and $A_3|\psi\rangle$.

Let us begin by noting that Eq. (47) for $i = 2$ gives us directly such a linear combination for $A_2|\psi\rangle$ and so $A_2|\psi\rangle \in V$. Then, the fact that $A_i|\psi\rangle \in V$ for $i = 4, \dots, n$ follows from Eq. (47); it is enough to rewrite the latter as

$$A_i|\psi\rangle = \frac{1-2\alpha}{\alpha}|\psi\rangle - \frac{1}{\alpha}A_{i-1}|\psi\rangle - A_{i-2}|\psi\rangle. \quad (85)$$

Let us now move on to showing that $A_i A_j|\psi\rangle \in V$ for all $i \neq j$. To this end, we first observe that using (48) we obtain

$$\begin{aligned} A_i A_{i\pm 1}|\psi\rangle &= (2P_i - \mathbb{1})(2P_{i\pm 1} - \mathbb{1})|\psi\rangle \\ &= -(A_i + A_{i\pm 1} + \mathbb{1})|\psi\rangle, \end{aligned} \quad (86)$$

which due to the fact that $A_i|\psi\rangle \in V$, allows us to conclude that for all i , $A_i A_{i\pm 1}|\psi\rangle \in V$.

Let us then consider the vectors $A_i A_j|\psi\rangle$ for pairs i, j such that $|i - j| = 2$. Using the property of involution and the fact $[A_i, A_{i\pm 1}]|\psi\rangle = 0$ which is a consequence of Eq. (48), we get

$$\begin{aligned} A_i A_{i\pm 2}|\psi\rangle &= A_i A_{i\pm 2}(A_{i\pm 1})^2|\psi\rangle \\ &= (A_i A_{i\pm 1})(A_{i\pm 1} A_{i\pm 2})|\psi\rangle. \end{aligned} \quad (87)$$

Since we have already shown $A_i A_{i\pm 1}|\psi\rangle \in V$, the above equation implies $A_i A_{i\pm 2}|\psi\rangle \in V$.

Given that $A_i A_j|\psi\rangle \in V$ for $|i - j| = 1$ and $|i - j| = 2$ we can then prove, applying the same argument as above, that $A_i A_j|\psi\rangle$ belong to V for any pair i, j such that $|i - j| = 3$. In fact, following this approach recursively we can prove that $A_i A_j|\psi\rangle \in V$ for i, j such that $|i - j| = k$ with $k = 3, \dots, n - 1$, which completes the proof. \square

Let us remark that the subspace V is in fact spanned by any triple of the vectors $|\psi\rangle$, $A_i|\psi\rangle$ and $A_j|\psi\rangle$ with $i \neq j$. This is a consequence of the fact that, as proven above, any vector $A_i|\psi\rangle$ is a linear combination of $|\psi\rangle$, $A_1|\psi\rangle$ and $A_3|\psi\rangle$.

Lemma 2. *If a set of projectors $\{\tilde{P}_i\}_{i=1}^n$ acting on \mathbb{C}^3 and a vector $|\tilde{\psi}\rangle$ satisfy the relations (51) and (52), then each \tilde{P}_i has rank one, that is, for each i there exists a normalized vector $|v_i\rangle \in \mathbb{C}^3$ such that $\tilde{P}_i = |v_i\rangle\langle v_i|$ and, moreover, $\langle v_i|v_{i\pm 1}\rangle = 0$.*

Proof. Since \tilde{P}_i are projectors, we have

$$\forall i, \tilde{P}_i^2|\tilde{\psi}\rangle = \tilde{P}_i|\tilde{\psi}\rangle. \quad (88)$$

Let us begin by showing that $\tilde{P}_i|\tilde{\psi}\rangle \neq 0$ for all i . Assume to this end that there exist j such that $\tilde{P}_j|\tilde{\psi}\rangle = 0$. Using then Eq. (52) for $i = j - 1$ we arrive at

$$(\tilde{P}_{j-1} + \alpha\tilde{P}_{j-2})|\tilde{\psi}\rangle = |\tilde{\psi}\rangle. \quad (89)$$

After applying \tilde{P}_{j-2} to both sides of this equation and using Eq. (51), we obtain $\alpha\tilde{P}_{j-2}^2|\tilde{\psi}\rangle = \tilde{P}_{j-2}|\tilde{\psi}\rangle$ which is consistent with Eq. (88) if and only if $\tilde{P}_{j-2}|\tilde{\psi}\rangle = 0$. Therefore, due to Eq. (89) we have $\tilde{P}_{j-1}|\tilde{\psi}\rangle = |\tilde{\psi}\rangle$. Again, substituting these relations in (52) taking $i = j$, we arrive at $\tilde{P}_{j+1}|\tilde{\psi}\rangle = [(1 - \alpha)/\alpha]|\tilde{\psi}\rangle$ which contradicts Eq. (88).

Let us now show that all the operators \tilde{P}_i are of rank one. We first prove that none of them can be of rank three. Assume for this purpose that $\text{rank}(\tilde{P}_j) = 3$ for some j . Then, the condition (88) gives $\tilde{P}_j|\tilde{\psi}\rangle = |\tilde{\psi}\rangle$. This, after taking into account that $\tilde{P}_{j+1}\tilde{P}_j|\tilde{\psi}\rangle = 0$ implies $\tilde{P}_{j+1}|\tilde{\psi}\rangle = 0$, which contradicts the fact $\tilde{P}_i|\tilde{\psi}\rangle \neq 0$ for all i , as shown before.

Let us then prove that none of \tilde{P}_i can be of rank two. To this end, assume that there is j such that $\text{rank}(\tilde{P}_j) = 2$ and consider the eigen-decomposition of \tilde{P}_j ,

$$\tilde{P}_j = |1\rangle\langle 1| + |2\rangle\langle 2|, \quad (90)$$

where $|1\rangle, |2\rangle, |3\rangle$ are the eigenvectors, forming an orthonormal basis in \mathbb{C}^3 . Subsequently, $|\tilde{\psi}\rangle$ can be expressed as

$$|\tilde{\psi}\rangle = x_1|1\rangle + x_2|2\rangle + x_3|3\rangle \quad (91)$$

for some $x_1, x_2, x_3 \in \mathbb{C}$. Note that $x_1 = x_2 = 0$ is not possible since it requires $\tilde{P}_j|\tilde{\psi}\rangle = 0$. Similarly, $x_3 \neq 0$, otherwise $\tilde{P}_j|\tilde{\psi}\rangle = |\tilde{\psi}\rangle$ which implies $\tilde{P}_{j\pm 1}|\tilde{\psi}\rangle = 0$.

Now, employing the fact that \tilde{P}_j is supported on $\text{span}\{|1\rangle, |2\rangle\}$, it follows from the condition $\tilde{P}_j\tilde{P}_{j\pm 1}|\tilde{\psi}\rangle = 0$ that $\tilde{P}_{j\pm 1}|\tilde{\psi}\rangle = q_{3,\pm}|3\rangle$ for some $q_{3,\pm} \in \mathbb{C}$. By combining this with (88) we find that

$$\tilde{P}_{j\pm 1}|3\rangle = |3\rangle, \quad (92)$$

that is, $|3\rangle$ is the eigenvector of $\tilde{P}_{j\pm 1}$ with eigenvalue one, which, due to the fact that $\tilde{P}_{j\pm 1} \leq \mathbb{1}$, implies that $\tilde{P}_{j\pm 1}$ decompose as

$$\tilde{P}_{j\pm 1} = \tilde{P}'_{j\pm 1} + |3\rangle\langle 3| \quad (93)$$

with $\tilde{P}'_{j\pm 1}$ being projectors supported on $\text{span}\{|1\rangle, |2\rangle\}$. By finally plugging Eqs. (90) - (93) into Eq. (52) for $i = j$ and projecting the obtained equation onto $|3\rangle$ we see that $2\alpha = 1$, which is not satisfied for any n .

As a result all the operators \tilde{P}_i are of rank one and therefore they can be expressed as

$$\tilde{P}_i = |v_i\rangle\langle v_i| \quad (94)$$

for some $|v_i\rangle \in \mathbb{C}^3$. Furthermore, since $\tilde{P}_i|\tilde{\psi}\rangle \neq 0$, Eq. (51) implies $\langle v_i|v_{i\pm 1}\rangle = 0$. This completes the proof. \square

Chapter 3

Paper II

3.1 Scalable noncontextuality inequalities and certification of multiqubit quantum systems

In the second article forming this thesis we continue our endeavour to provide certification methods for quantum systems. This time our main aim was to provide methods that unlike the n -cycle inequalities discussed above allow to certify systems of arbitrary dimension. However, due to the complexity of the problem we needed to restore to the standard contextuality scenario in which one needs to assume that the underlying compatibility structure of measurements is satisfied. This means that our method falls into the category of semi-device independent methods.

In this article we proposed a family of noncontextuality inequalities that involve $2n$ dichotomic measurements with n being an arbitrary natural number such that $n \geq 3$. In the particular case of three qubits, our family reproduces an inequality that in the non-locality context is known as the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality [88]-[89], however, for larger values of n both classes are distinct.

To construct these inequalities, but also to derive our main results stated in Theorems 1 and 2, we employed the stabilizer formalism which in fact has already proven to be very useful for instance in deriving Bell inequalities for multipartite states (see, e.g., Ref. [64]). Our inequalities are constructed in such a way that their maximal quantum violation is achieved by an n -qubit state equivalent to the GHZ state (1.45) and a set of observables that form anticommuting pairs, this being a key fact behind the possibility of using these inequalities for certification of quantum states and measurements.

Indeed, we then prove that the only possible quantum realizations (consisting of quantum states and measurements) that achieve the maximal quantum violation of our inequalities are those that are unitarily equivalent to the one specified above in the sense of Def. 15. Thus, the maximal violation of our inequalities certifies that the underlying state is equivalent to the GHZ state of n qubits (1.45) and simultaneously the observables are equivalent to n pairs of anticommuting observables, which are in fact, equivalent to pairs of the Pauli matrices X and Z acting on all subsystems of this state. In deriving this result, the structure of the compatibility hypergraph in the simplest case of $n = 3$ played a key role because it allowed to identify relevant symmetries of the inequality which then simplified the algebraic relations for the observables, but it also allowed to generalize the inequality to the case of arbitrary n . Finally, following the approach of Ref. [68], in the simplest case of $n = 3$ we have also

studied the robustness of our scheme against noises and experimental imperfections.




The key feature of our inequalities is that they are scalable in the sense that the number of expectation values that they involve scales only polynomially with the system size n . This certainly lowers the experimental effort necessary to violate them as compared to other such inequalities like the aforementioned MAKBB inequalities which contain 2^n terms.

3.2 Author's contribution

My contribution to the article consisted of:

- Active participation in the discussion that led to formulation of the problem and derivation of the noncontextuality inequalities;
- Generalization of the inequalities to any n based on the inequality for $n = 3$. In deriving these inequalities I exploited the symmetries of the underlying compatibility hypergraph;
- Proving Lemmas 1, 2 and 3 and as a consequence Theorem 1;
- Significant contribution to proving Lemmas 4, 5 and 6 and Theorem 2;
- Help in deriving the robustness analysis presented in Sec. V of the article;
- Significant contribution to writing the manuscript.

Scalable noncontextuality inequalities and certification of multiqubit quantum systems

Rafael Santos , Chellasamy Jebarathinam , and Remigiusz Augusiak 

Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland



(Received 20 February 2022; accepted 28 June 2022; published 25 July 2022)

We propose a family of noncontextuality inequalities and show that they can be used for certification of multiqubit quantum systems. Our scheme, unlike those based on nonlocality, does not require spatial separation between the subsystems, yet it makes use of certain compatibility relations between measurements. Moreover, it is scalable in the sense that the number of expectation values that are to be measured to observe contextuality scales polynomially with the number of qubits that are being certified. In a particular case we also show our scheme to be robust to errors and experimental imperfections. Our results seem promising as far as certification of physical setups is concerned in scenarios where spatial separation between the subsystems cannot be guaranteed.

DOI: [10.1103/PhysRevA.106.012431](https://doi.org/10.1103/PhysRevA.106.012431)

I. INTRODUCTION

Multiqubit entangled states constitute a key resource for various quantum information tasks such as quantum computation [1,2] and error correction [3,4], quantum communication [5,6], quantum simulations [7,8], and cryptographic protocols [9,10]. To realize genuine quantum technologies employing such tasks, the back-end user should be guaranteed that the quantum devices work as specified by the provider. The standard state verification schemes based on quantum tomography [11,12], however, suffer from two problems: they are unfeasible for larger systems and require using trusted and well-characterized measuring devices.

Observing nonclassical correlations through the violation of a Bell-type inequality [13] can be used to detect entanglement in a device-independent way; i.e., it implies the presence of entanglement without the need to have a trust in the measurement devices. This property of the violation of Bell inequalities makes them a useful resource for implementing quantum information protocols such as quantum key distribution in a device-independent way [14]. Remarkably, maximal quantum violation of certain Bell inequalities can be used to demonstrate a phenomenon called “self-testing of quantum states and measurements” [15,16], which can be used to provide device-independent characterization of quantum devices. Recently, such a form of certification based on the phenomenon of nonlocality has been explored extensively. For instance, several self-testing statements for multiqubit graph states were recently derived in Refs. [17–19]. However, genuine demonstration of the violation of Bell inequalities requires a spatial separation between the subsystems.

Sequential quantum measurements on a single system can be used to observe quantum contextuality [20] and temporal quantum correlations [21–23] through the violation of suitable inequalities. Apart from the foundational relevance of these two notions of nonclassicality, on one side, they have been explored as a resource for quantum information applications such as measurement-based quantum computation [24–27]. On the other side, they have also been used for certification of relevant quantum properties such as the

dimension of the underlying quantum system [28,29]. More importantly, contextuality and temporal correlations have also been exploited for certification of quantum states and/or measurements [30–34].

Motivated by the above results, in this work we introduce a family of noncontextuality inequalities that are maximally violated by many-qubit quantum systems and certain pairs of anticommuting observables. In constructing our inequalities we exploit the multiqubit stabilizer formalism known for its use in quantum error correction [35–37]. These inequalities are scalable in the sense that the number of expectation values they are built from scales polynomially with the number of observables, $2n$, that are measured; yet their maximal violation can be achieved by quantum systems of dimension at least 2^n . From this point of view they can be seen as dimension witnesses. In the particular case $n = 3$ our family reproduces an inequality that in the nonlocality context is known as the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality [38–40] (see also Refs. [41–43] for other approaches to reveal Bell nonlocality or quantum contextuality based on stabilizer formalism). Yet for $n > 3$ these families are distinct. We then show that our inequalities can be used for certification of multiqubit quantum systems in the sense of Ref. [32]. In fact, we generalize the results of that work to any number of qubits.

Our work is organized as follows. In Sec. II we outline the contextuality scenario and provide the definitions of graph states and self-testing. In Sec. III we present the simplest inequality designed to certify the three-qubit graph state corresponding to the complete graph together with three pairs of anticommuting observables. In Sec. IV we present a scalable family of inequalities designed to certify multiqubit quantum systems. In Sec. V we investigate whether our certification schemes are robust.

II. PRELIMINARIES

We begin by illustrating our scenario and introducing the relevant notations and definitions.

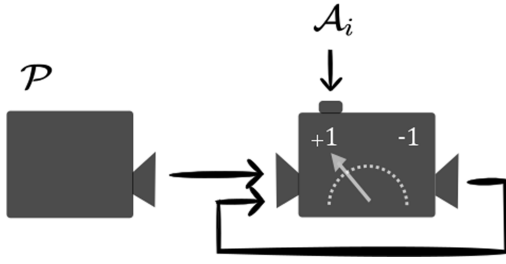


FIG. 1. Measurement setup. A contextuality experiment comprises of a preparation device \mathcal{P} that prepares some quantum state ρ which is later measured sequentially by the nondemolishing measurement device with settings A_i ; each of these measurements yields the ± 1 outcome. Figure from Ref. [33].

A. Contextuality scenario

A standard contextuality scenario is defined by a triple of sets: a set of measurements, a set of outcomes of the measurements, and a set of contexts, which are the subsets of compatible measurements. The notion of compatibility in a contextuality scenario means that the measurements that belong to the same context can be performed jointly or in a sequence in such a way that the observed statistics are independent of the order in which these measurements were performed. In the latter case, however, the measurements are nondemolishing, meaning that they do not physically destroy the system.

Each run of the experimental observation comprises of preparation of a physical system followed by a sequence of nondemolishing measurements in a device as depicted in Fig. 1. The measurement device has no memory and returns only the actual postmeasurement state. The measurement device has different settings, each of which yields two outcomes which we label by ± 1 . The contexts will be defined in the specific scenarios studied. Let us stress here that in the quantum case the above scenario comprises the most general situation in which the physical system is described by a mixed state and the measurements need not be projective.

After repeating this experiment many times, one estimates the joint probabilities of obtaining the outcomes of measurements that are performed on the preparation and, consequently, their correlation functions, which are average values over the outcomes of the measurements. For instance, if the measurements A_1 , A_2 , and A_3 , which belong to the same context, are performed in sequence or jointly, we can estimate the 2^3 joint probabilities $p(a_1, a_2, a_3 | A_1, A_2, A_3)$ as well as the correlation function

$$\langle A_1 A_2 A_3 \rangle = \sum_{a_i = \pm 1} a_1 a_2 a_3 p(a_1, a_2, a_3 | A_1, A_2, A_3). \quad (1)$$

This notation can be naturally extended to any sets of compatible measurements.

To reveal contextuality in the experiment one typically uses noncontextuality inequalities as violation of such inequalities by the joint probabilities implies that any noncontextual hidden variable model cannot reproduce them [20]. Typically such inequalities are defined in terms of linear expressions composed of correlation functions. For instance, in a scenario where the measurements are performed in triples, we can

consider the following form of inequality:

$$\mathcal{I} := \sum_{i,j,k} c_{i,j,k} \langle A_i A_j A_k \rangle \leq \eta_C \leq \eta_Q, \quad (2)$$

where $c_{i,j,k}$ are real coefficients to be chosen, and η_C and η_Q are the classical and quantum bounds.

If there is a noncontextual hidden variable model that describes the joint probabilities, then the inequality with the classical bound η_C is satisfied. Here, the meaning of classicality is mathematically defined as the existence of a noncontextual hidden variable model, for which the expectation values in Eq. (2) factorize and each individual expectation value is deterministic, i.e., $\langle A_i A_j A_k \rangle = a_i a_j a_k$, with $a_i \in \{+1, -1\}$. Consequently, the classical bound η_C of Eq. (2) can be derived as the maximum value that can be attained by any such model,

$$\eta_C = \max_{a_i = \pm 1} \left(\sum_{i,j,k} c_{i,j,k} a_i a_j a_k \right). \quad (3)$$

On the other hand, the quantum bound of the inequality is defined as the optimal value of the linear expression obtained over all the possible quantum states and measurements in any Hilbert space. Since we do not specify the dimension of the underlying Hilbert space, without any loss of generality, we can assume that the measurements are projective and the state is pure (see, e.g., Ref. [32], where an extension of the Neumark dilation theorem is proven). In other words, any correlations obtained within the above experiment can always be reproduced with a pure state and projective measurements satisfying the same compatibility relations.

For instance, in the case of the inequality given in Eq. (2) the quantum bound is evaluated to be

$$\eta_Q = \sup_{A_i: \rho} \left[\sum_{i,j,k} c_{i,j,k} \text{tr}(\rho A_i A_j A_k) \right], \quad (4)$$

where the observables A_i are Hermitian operators acting on a Hilbert space \mathcal{H} and satisfying $A_i^2 = \mathbb{1}$ for any i and $\rho = |\psi\rangle\langle\psi|$ is some pure state that describes the preparation.

Our aim here is to introduce certain noncontextuality inequalities that are scalable in the sense that the number of expectation values they consist of grows polynomially with n and, at the same time, their maximal violation can be achieved only by quantum systems of dimension 2^n . We also explore whether these inequalities can be used for certification of quantum states and measurements.

B. Graph states

A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a mathematical object defined by a set of vertices \mathcal{V} and a set of edges \mathcal{E} that connect some pairs of vertices. By $\mathcal{N}(i)$ we denote the neighborhood of the vertex i , that is, a set of those vertices that are connected to i by an edge. Also, we call a graph connected if any two vertices are connected by a path composed of edges.

Interestingly, one can exploit the notion of a graph to define classes of pure entangled multipartite states. While in principle there are many ways of doing that, here we follow the definition based on the stabilizer formalism [44] (see also

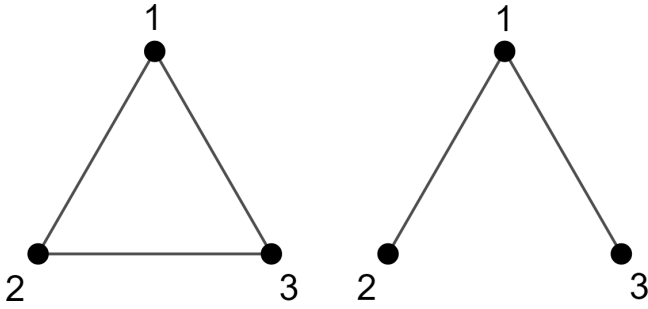


FIG. 2. Two nonisomorphic graphs with three vertices.

Ref. [45] for a review on graph states). It allows one to associate an N -qubit entangled state to any connected N -vertex graph \mathcal{G} .

In order to present the construction consider the Pauli matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (5)$$

Now, to each vertex $i \in \mathcal{V}$ one associates an N -qubit operator G_i defined as

$$G_i = X_i \otimes \bigotimes_{j \in \mathcal{N}(i)} Z_j, \quad (6)$$

where the single X acts on site i , whereas the Z operators act on all sites that belong to the neighborhood $\mathcal{N}(i)$ of i . Having introduced the G_i operators we define the graph state.

Definition 1. We define the graph state $|G\rangle$ associated to the graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ as the unique state stabilized by the corresponding operators G_i (6), that is,

$$G_i |G\rangle = |G\rangle, \quad \forall i = 1, \dots, N. \quad (7)$$

In other words, $|G\rangle$ is the unique common eigenstate of all G_i corresponding to eigenvalue $+1$.

The operators G_i are usually called the stabilizing operators. Notice also that they mutually commute and the Abelian group generated by them is called a stabilizer.

Two simple examples of connected graphs with three vertices are depicted in Fig. 2. The graph on the left is a complete graph, i.e., one in which any vertex is connected to any other vertex by an edge. The unique three-qubit state associated to this graph is stabilized by the following three stabilizing operators,

$$G_1 = X \otimes Z \otimes Z, \quad (8)$$

$$G_2 = Z \otimes X \otimes Z, \quad (9)$$

$$G_3 = Z \otimes Z \otimes X, \quad (10)$$

and can be stated as

$$|G'\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |100\rangle + |010\rangle - |110\rangle + |001\rangle - |101\rangle - |011\rangle - |111\rangle). \quad (11)$$

The graph on the right-hand side in Fig. 2 is nonisomorphic to the complete graph. The unique three-qubit state associated with this graph is stabilized by

$$G_1 = X \otimes Z \otimes Z, \quad (12)$$

$$G_2 = Z \otimes X \otimes \mathbb{1}, \quad (13)$$

$$G_3 = Z \otimes \mathbb{1} \otimes X, \quad (14)$$

and is given by

$$|G''\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |100\rangle + |010\rangle - |110\rangle + |001\rangle + |101\rangle - |011\rangle + |111\rangle). \quad (15)$$

Let us notice that although both these exemplary states $|G'\rangle$ and $|G''\rangle$ correspond to nonisomorphic graphs, they are actually equivalent to the same three-qubit Greenberger-Horne-Zeilinger (GHZ) state,

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \quad (16)$$

by suitable local unitary transformations.

In the context of multipartite qubit states such a vertex is associated to a qubit and edges represent entanglement between qubits. However, in our scheme that we propose for certification of such a multiqubit state, we do not assume that there exists a local Hilbert space corresponding to each vertex.

Let us finally notice that the construction of the graph state corresponding to the three-vertex complete graph can be generalized to any number of qubits. The corresponding stabilizing operators are given by

$$G_i = Z_1 \cdots Z_{i-1} X_i Z_{i+1} \cdots Z_n, \quad (17)$$

with $i = 1, \dots, n$. They stabilize an n -qubit graph state that is local-unitary equivalent to the GHZ state $(1/\sqrt{2})(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$.

C. Self-testing

Self-testing, originally defined in Ref. [15] in the context of nonlocality, aims to certify an unknown quantum state and a set of measurements based on statistics obtained in an experiment, up to certain unitary equivalence and the existence of auxiliary degrees of freedom. Self-testing based on violation of Bell inequalities is by definition a device-independent task as it does not depend on any assumption on the state and measurements. In a Bell test, the assumption of commutativity between the measurements arises due to the fact that spatially separated subsystems cannot communicate instantaneously with each other.

Self-testing statements based on violation of noncontextuality inequalities require, on the other hand, the assumption of compatibility of measurements. First, contextuality-based self-testing was defined in Ref. [31] in a similar way to how self-testing is defined within the Bell scenario. Here we provide a slightly different definition that takes inspiration from Ref. [32] (see also Ref. [33]) and fits better the inequalities introduced here.

To this aim, let us consider again the experiment described in Sec. II A, but now we assume that both the state (in general mixed) and measurements (in general nonprojective) are unknown; still, the measurements obey certain compatibility relations. Since we do not specify the dimension of the underlying Hilbert space, without loss of generality, we can assume that the measurements are projective and the state is pure (see, e.g., Ref. [32]). In other words, any correlations giving rise to the violation of the noncontextuality inequality can always be reproduced with a pure state $\rho = |\psi\rangle\langle\psi|$ and observables A_i obeying $A_i^2 = \mathbb{1}$, all acting on some Hilbert space of unknown dimension \mathcal{H} . These observables obey the same compatibility relations.

At the same time we consider a reference experiment with a known pure state $|\tilde{\psi}\rangle \in \mathbb{C}^d$ for some d and known observables \tilde{A}_i acting on \mathbb{C}^d that obey the same compatibility relations.

Definition 2. Suppose an unknown state $|\psi\rangle \in \mathcal{H}$ and a set of measurements A_i violate a given noncontextuality inequality maximally; then this maximal quantum violation self-tests the state $|\tilde{\psi}\rangle \in \mathbb{C}^d$ and the set of measurements \tilde{A}_i if there exists a projection $P : \mathcal{H} \rightarrow \mathbb{C}^d$ and a unitary U acting on \mathbb{C}^d such that

$$U^\dagger(P A_i P^\dagger)U = \tilde{A}_i, \quad (18)$$

$$U(P|\psi\rangle) = |\tilde{\psi}\rangle. \quad (19)$$

Speaking alternatively, the above definition says that based on the observed nonclassicality one is able to identify a subspace $V = \mathbb{C}^d$ in \mathcal{H} on which all the observables act invariantly. Equivalently, A_i can be decomposed as $A_i = \hat{A}_i \oplus A'_i$, where \hat{A}_i act on V , whereas A'_i act on the orthocomplement of V in \mathcal{H} ; in particular, $A'_i|\psi\rangle = 0$. Moreover, there is a unitary $U^\dagger \hat{A}_i U = \tilde{A}_i$.

III. THE SIMPLEST INEQUALITY AND SELF-TESTING OF THREE-QUBIT GRAPH STATE

A. Simplest inequality

Here, we consider a noncontextuality inequality that allows for self-testing the complete graph state of three qubits and simultaneously a set of six dichotomic observables denoted by A_i and B_j ($i, j \in \{1, 2, 3\}$) such that $\{A_i, B_i\} = 0$ ($i = 1, 2, 3$). The measurement outcomes are labeled by ± 1 , which means that the measurement operators have eigenvalues ± 1 and thus they satisfy $A_i^2 = B_i^2 = \mathbb{1}$.

The compatibility hypergraph of the scenario is depicted in Fig. 3. A compatibility hypergraph is one in which the vertices are associated with the measurements of the scenario and the hyperedges represent the contexts which are subsets of compatible measurements. The noncontextuality inequality we consider is given by

$$\begin{aligned} \mathcal{I}_3 &:= \langle A_1 B_2 B_3 \rangle + \langle B_1 A_2 B_3 \rangle + \langle B_1 B_2 A_3 \rangle - \langle A_1 A_2 A_3 \rangle \\ &\leq \eta_C = 2 < \eta_Q = 4. \end{aligned} \quad (20)$$

The above inequality is equivalent to a noncontextuality inequality employed in Ref. [46] to demonstrate quantum contextuality of a single eight-dimensional quantum system. In the context of the Bell scenario it is the well-known MABK

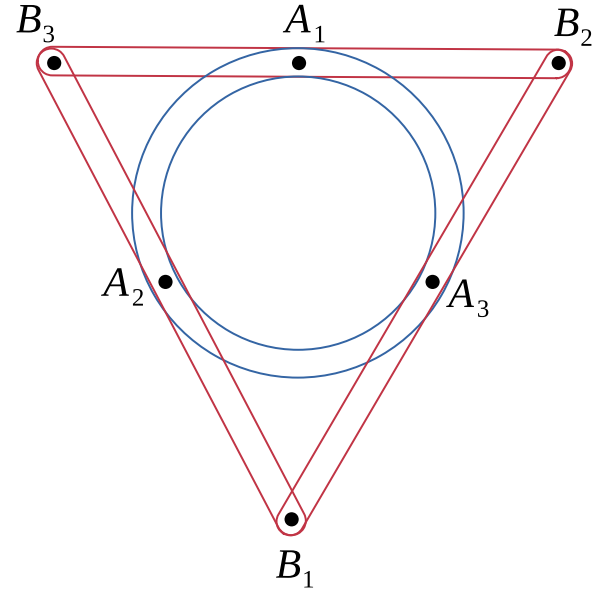


FIG. 3. Hypergraph [47] of compatibility of the Kochen-Specker contextuality scenario associated to inequality (20). In this hypergraph, the vertices represent the observables of the scenario and the hyperedges represent the contexts. The red hyperedges are associated to the correlators which enter inequality (20) with $+1$ and the blue to correlators corresponding to the negative sign. Here the colors are conveniently chosen in order to elucidate symmetric properties of the inequality.

inequality [38–40] for which a non-locality-based self-testing statement was derived in Ref. [17].

Following the argument in the previous section, the classical bound of the above expression can be obtained by assigning the values ± 1 to each variable A_i and B_j which implies $\eta_C = 2$. At the same time, the algebraic maximum of \mathcal{I}_3 is four since the correlators can take a value between -1 and $+1$, and, importantly, it equals the maximal quantum value of \mathcal{I}_3 , that is, $\eta_Q = 4$. Indeed, it can be checked that the following set of measurements,

$$\begin{aligned} A_1 &= X \otimes \mathbb{1} \otimes \mathbb{1}, & B_1 &= Z \otimes \mathbb{1} \otimes \mathbb{1}, \\ A_2 &= \mathbb{1} \otimes X \otimes \mathbb{1}, & B_2 &= \mathbb{1} \otimes Z \otimes \mathbb{1}, \\ A_3 &= \mathbb{1} \otimes \mathbb{1} \otimes X, & B_3 &= \mathbb{1} \otimes \mathbb{1} \otimes Z, \end{aligned} \quad (21)$$

together with the complete graph state $|G'\rangle$ given by Eq. (11) give rise to the algebraic maximum. This follows from the fact that for this choice of observables, the first three terms of the inequality correspond to the stabilizing operators G_i given in Eq. (8), whereas the last one corresponds to their product $G_1 G_2 G_3 = -X_1 X_2 X_3$.

Let us notice that almost all pairs of these observables commute except for those with the same subscripts which anticommute, that is,

$$[A_i, A_j] = [A_i, B_j] = [B_i, B_j] = 0 \quad (i \neq j) \quad (22)$$

and

$$\{A_i, B_i\} = 0 \quad (i = 1, 2, 3). \quad (23)$$

For further convenience let us also comment on the symmetries of inequality (20). A simple way to visualize these symmetries is by using the compatibility hypergraph of the scenario that is represented in Fig. 3. For instance, note that under the relabeling of the measurements $A_i \leftrightarrow A_j$ together with $B_i \leftrightarrow B_j$, i.e., a permutation of subscripts $i \leftrightarrow j$, the inequality remains the same. We can also observe that a cyclic permutation of measurements $A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow A_1$ together with $B_3 \rightarrow B_1 \rightarrow B_2 \rightarrow B_3$ does not change the structure of the hypergraph and therefore the inequality remains the same. Other symmetries can be found just by looking at the hypergraph since it captures the intrinsic structure of the associated inequality. The above symmetries as well as the structure of the \mathcal{I}_3 expression will be vital for our considerations, in particular, for generalizing this inequality into a family of inequalities maximally violated by n -qubit GHZ states and n pairs of anticommuting observables.

B. Self-testing

We now prove that the maximal quantum violation of inequality (20) can be used for certification of the GHZ state (11) along with the observables (21). To this aim, consider a quantum realization given by a pure state $|\psi\rangle \in \mathcal{H}$ and a set of quantum observables A_i, B_j with $i, j = 1, 2, 3$ acting on \mathcal{H} , where \mathcal{H} is some unknown Hilbert space. We additionally assume that these observables obey the compatibility relations presented in Fig. 3, which translate into the commutation relations in Eq. (22).

Assume then the correlations obtained by measuring A_i and B_j on the state $|\psi\rangle$ attain the quantum bound of inequality (20). This directly implies that the first three terms in \mathcal{I}_3 take value 1, whereas the last term equals -1 , which via the Cauchy-Schwarz inequality translate to the following equations:

$$A_1 B_2 B_3 |\psi\rangle = |\psi\rangle \quad \text{and permutations,} \quad (24)$$

$$B_1 A_2 B_3 |\psi\rangle = |\psi\rangle \quad \text{and permutations,} \quad (25)$$

$$B_1 B_2 A_3 |\psi\rangle = |\psi\rangle \quad \text{and permutations,} \quad (26)$$

$$A_1 A_2 A_3 |\psi\rangle = -|\psi\rangle \quad \text{and permutations,} \quad (27)$$

where “permutations” refers to the fact that the above relations also hold if we permute the observables, which is a consequence of the commutation relations (22). One directly deduces from these identities that

$$\begin{aligned} A_1 B_1 |\psi\rangle &= A_1 A_2 B_3 |\psi\rangle = -B_3 A_3 |\psi\rangle \\ &= A_1 A_3 B_2 |\psi\rangle = A_3 B_3 |\psi\rangle, \end{aligned} \quad (28)$$

where in the first line we used $B_1 |\psi\rangle = A_2 B_3 |\psi\rangle$ from Eq. (25) and then the fact that B_3 commutes with A_1 and A_2 along with the relation $A_1 A_2 |\psi\rangle = -A_3 |\psi\rangle$ that stems from Eq. (27). On the other hand, in the second line, we used $B_1 |\psi\rangle = A_3 B_2 |\psi\rangle$ from Eq. (26) and $A_1 B_2 |\psi\rangle = A_3 |\psi\rangle$ from Eq. (27).

Let us now employ the symmetries of the inequality. Indeed, as already mentioned, it is invariant under simultaneous permutations $A_i \leftrightarrow A_j$ and $B_i \leftrightarrow B_j$ for any $i \neq j$, and therefore one can straightforwardly infer from Eq. (28) that the

following chain of equalities holds true:

$$\begin{aligned} A_1 B_1 |\psi\rangle &= A_2 B_2 |\psi\rangle = A_3 B_3 |\psi\rangle \\ &= -B_1 A_1 |\psi\rangle = -B_2 A_2 |\psi\rangle = -B_3 A_3 |\psi\rangle. \end{aligned} \quad (29)$$

From the above equations it follows that the operators A_i and B_i with $i = 1, 2, 3$ anticommute when acting on the state $|\psi\rangle$, i.e.,

$$\{A_i, B_i\} |\psi\rangle = \{A_2, B_2\} |\psi\rangle = \{A_3, B_3\} |\psi\rangle = 0. \quad (30)$$

Inspired by the approach of Ref. [32], we now define a subspace

$$\begin{aligned} V &:= \text{span}\{|\psi\rangle, A_1 |\psi\rangle, A_2 |\psi\rangle, A_3 |\psi\rangle, \\ &\quad B_1 |\psi\rangle, B_2 |\psi\rangle, B_3 |\psi\rangle, A_1 B_1 |\psi\rangle\}, \end{aligned} \quad (31)$$

and prove the following fact for it.

Lemma 1. V is an invariant subspace of all the observables A_i and B_j for $i, j \in \{1, 2, 3\}$.

Proof. One can verify with the aid of Eqs. (24)–(27) that the action of the operator A_1 on the eight vectors spanning V is a permutation of these vectors up to the factor -1 . In exactly the same way, one shows that $B_1 V \subseteq V$. Therefore, we conclude that the subspace V is invariant under the action of the observables A_1 and B_1 . By the symmetry of inequality (20) it then follows that the subspace V is invariant under the action of all observables A_i and B_j for $i, j \in \{1, 2, 3\}$. ■

It should be noticed that due to Eq. (29), the subspace V stays the same if one replaces the last vector $A_1 B_1 |\psi\rangle$ in Eq. (31) by $A_2 B_2 |\psi\rangle$ or $A_3 B_3 |\psi\rangle$.

Due to Lemma 1, it suffices for our purpose to identify the form of the state $|\psi\rangle$ and the operators A_i and B_j restricted to the subspace V . In fact, the whole Hilbert space splits as $\mathcal{H} = V \oplus V^\perp$, where V^\perp is an orthocomplement of V in \mathcal{H} . Then, the fact that V is an invariant subspace of all the observables A_i and B_j means that they have the following block structure:

$$A_i = \hat{A}_i \oplus A'_i, \quad B_j = \hat{B}_j \oplus B'_j, \quad (32)$$

where $\hat{A}_i = P A_i P$ and analogously $\hat{B}_i = P B_i P$ with $P : \mathcal{H} \rightarrow V$ being a projection onto V . Since A'_i and B'_j act trivially on V , that is, $A'_i V = B'_j V = 0$, which means that the observed correlations giving rise to the maximal violation of inequality (20) come solely from the subspace V , in what follows we can restrict our attention to the operators \hat{A}_i and \hat{B}_j .

First, from the fact that A_i and B_j are observables obeying $A_i^2 = B_j^2 = \mathbb{1}$, it directly follows that \hat{A}_i, \hat{B}_j are observables too and satisfy

$$\hat{A}_i^2 = \hat{B}_j^2 = \mathbb{1}_V \quad (i, j = 1, 2, 3), \quad (33)$$

where $\mathbb{1}_V$ is the identity acting on V . Second, Eq. (32) implies that the hatted observables must obey the same commutation relations as A_i and B_j , that is,

$$[\hat{A}_i, \hat{A}_j] = [\hat{A}_i, \hat{B}_j] = [\hat{B}_i, \hat{B}_j] = 0 \quad (i \neq j). \quad (34)$$

Third, it turns out that relations (30) force \hat{A}_i and \hat{B}_i to anticommute on the subspace V .

Lemma 2. Suppose the maximal quantum violation of inequality (20) is observed. Then, $\{\hat{A}_i, \hat{B}_i\} = 0$ for all $i \in \{1, 2, 3\}$.

Proof. Let us focus on the first pair \hat{A}_1 and \hat{B}_1 . By checking the action of $\{A_1, B_1\}$ on all the eight vectors that span the subspace V we can conclude that $\{\hat{A}_1, \hat{B}_1\} = 0$. Indeed, Eq. (30) implies that $\{A_1, B_1\}$ vanishes when acting on $|\psi\rangle$. Then, for $A_1|\psi\rangle$ one has

$$\{A_1, B_1\}A_1|\psi\rangle = (A_1B_1A_1 + B_1)|\psi\rangle = 0, \quad (35)$$

where the second equality follows again from Eq. (30). For $A_2|\psi\rangle$ and $A_3|\psi\rangle$ we can use the fact that A_1 and B_1 commute with A_2 and A_3 , which gives

$$\{A_1, B_1\}A_i|\psi\rangle = A_i\{A_1, B_1\}|\psi\rangle = 0 \quad (i = 2, 3). \quad (36)$$

In exactly the same way one deals with the vectors $B_i|\psi\rangle$. Finally, for the last vector in Eq. (31), $A_1B_1|\psi\rangle$, one has

$$\{A_1, B_1\}A_1B_1|\psi\rangle = (A_1B_1A_1B_1 + \mathbb{1})|\psi\rangle = 0, \quad (37)$$

where to get the last equality we use Eq. (30). Owing to the block form of A_1 and B_1 in Eq. (32), all this implies that $\{\hat{A}_1, \hat{B}_1\} = 0$.

One more time, by the symmetries of the inequality, we can draw the same conclusions for the remaining pairs of the observables A_i and B_i . As a result $\{\hat{A}_i, \hat{B}_i\} = 0$ for $i = 1, 2, 3$, which completes the proof. ■

With Lemma 2 at hand, we can now employ the standard approach that has already been used in many non-locality-based self-testing schemes [17,18,48,49]. Precisely, using this approach we can first infer that the dimension d of the subspace V is even. To see this, note that from the above anticommutation relation between \hat{A}_i and \hat{B}_i we have

$$\hat{A}_i = -\hat{B}_i\hat{A}_i\hat{B}_i \quad \text{or} \quad \hat{B}_i = -\hat{A}_i\hat{B}_i\hat{A}_i, \quad (38)$$

which after taking trace on both sides simplifies to $\text{tr}(\hat{A}_i) = \text{tr}(\hat{B}_i) = 0$. It then follows that both the eigenvalues ± 1 of each observable \hat{A}_i or \hat{B}_i have equal multiplicities. This clearly implies that the dimension $d = \dim V$ is an even number, $d = 2k$ for some $k \in \mathbb{N}$, and thus $V = \mathbb{C}^2 \otimes \mathbb{C}^k$. On the other hand, since $\dim V \leq 8$, one concludes that $k = 2, 3, 4$.

The fact that \hat{A}_1 and \hat{B}_1 are traceless means also that the operators \hat{A}_1 and \hat{B}_1 are equivalent to $X \otimes \mathbb{1}_k$ and $Z \otimes \mathbb{1}_k$ for some $k = 2, 3, 4$ up to some unitary operation (see for instance Appendix B in Ref. [48] for the proof of this statement). This observation is one of the key ideas behind the proof of the following lemma.

Lemma 3. Suppose the maximal quantum violation of inequality (20) is observed. Then, there exists a basis in V such that

$$\begin{aligned} \hat{A}_1 &= X \otimes \mathbb{1} \otimes \mathbb{1}, & \hat{B}_1 &= Z \otimes \mathbb{1} \otimes \mathbb{1}, \\ \hat{A}_2 &= \mathbb{1} \otimes X \otimes \mathbb{1}, & \hat{B}_2 &= \mathbb{1} \otimes Z \otimes \mathbb{1}, \\ \hat{A}_3 &= \mathbb{1} \otimes \mathbb{1} \otimes X, & \hat{B}_3 &= \mathbb{1} \otimes \mathbb{1} \otimes Z. \end{aligned} \quad (39)$$

Proof. First, from Lemma 2 we have $\{\hat{A}_1, \hat{B}_1\} = 0$ which implies that there exists a unitary U_1 acting on V such that

$$U_1^\dagger \hat{A}_1 U_1 = X \otimes \mathbb{1}_k, \quad (40)$$

$$U_1^\dagger \hat{B}_1 U_1 = Z \otimes \mathbb{1}_k, \quad (41)$$

where, as already mentioned, the dimension d of the subspace V is given by $d = 2k$ for some $k = 2, 3, 4$. Using then the

above form of \hat{A}_1 and \hat{B}_1 and the commutation relations (22) we can write the other operators as follows:

$$U_1^\dagger \hat{A}_2 U_1 = \mathbb{1}_2 \otimes M, \quad (42)$$

$$U_1^\dagger \hat{B}_2 U_1 = \mathbb{1}_2 \otimes N, \quad (43)$$

$$U_1^\dagger \hat{A}_3 U_1 = \mathbb{1}_2 \otimes O, \quad (44)$$

$$U_1^\dagger \hat{B}_3 U_1 = \mathbb{1}_2 \otimes P, \quad (45)$$

where M, N, O , and P are Hermitian involutions acting on the subspace of dimension k . To show explicitly how the above equations are obtained let us focus on \hat{A}_2 ; the proof for the other observables is basically the same. Since \hat{A}_2 acts on $\mathbb{C}^2 \otimes \mathbb{C}^k$, it can be decomposed in the Pauli basis as

$$U_1^\dagger \hat{A}_2 U_1 = \mathbb{1}_2 \otimes M_1 + X \otimes M_2 + Y \otimes M_3 + Z \otimes M_4, \quad (46)$$

where Y is the third Pauli matrix and M_i are some Hermitian matrices acting on \mathbb{C}^k . Now, it follows from the fact that \hat{A}_2 commutes with \hat{A}_1 , that $M_3 = M_4 = 0$. Then, from $[\hat{A}_2, \hat{B}_1]$ one obtains that $M_2 = 0$, and, by putting $M_1 = M$, we arrive at Eq. (42).

Second, from Lemma 2, we have $\{\hat{A}_2, \hat{B}_2\} = 0$ which is equivalent to $\{M, N\} = 0$. Since both M and N are involutions, one concludes, as before, that $k = 2k'$ for $k' = 1, 2$, or, equivalently, that $\mathbb{C}^k = \mathbb{C}^2 \otimes \mathbb{C}^{k'}$. Moreover, there exists another unitary transformation $U_2 : \mathbb{C}^k \rightarrow \mathbb{C}^k$ such that

$$U_2^\dagger M U_2 = X \otimes \mathbb{1}_{k'}, \quad (47)$$

$$U_2^\dagger N U_2 = Z \otimes \mathbb{1}_{k'}. \quad (48)$$

Finally, to learn the form of O and P we can again employ the commutation relations (22). They imply in particular that $[M, O] = [N, O] = [M, P] = [N, P] = 0$, and consequently,

$$O = \mathbb{1}_2 \otimes O', \quad P = \mathbb{1}_2 \otimes P', \quad (49)$$

where O' and P' are some operators acting on $\mathbb{C}^{k'}$ such that $[O']^2 = [P']^2 = \mathbb{1}_{k'}$. Additionally, due to the fact that $\{\hat{A}_3, \hat{B}_3\} = 0$, they must anticommute, $\{O', P'\} = 0$. This means that $k' = 2$ and that there exists a unitary operation U_3 acting on this qubit Hilbert space such that

$$U_3^\dagger O' U_3 = X, \quad U_3^\dagger P' U_3 = Z. \quad (50)$$

Taking all this into account, one finds that $V \cong \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ and that there exists a single unitary operation $U = U_1(\mathbb{1}_2 \otimes U_2)(\mathbb{1}_2 \otimes \mathbb{1}_2 \otimes U_3)$ on V which brings all the observables \hat{A}_i and \hat{B}_i to the form in Eqs. (39). ■

We have thus arrived at one of our main results of this paper.

Theorem 1. If a quantum state $|\psi\rangle$ and a set of measurements A_i and B_j with $i, j \in \{1, 2, 3\}$ maximally violate inequality (20), then there exist a projection $P : \mathcal{H} \rightarrow V$ with $V = (\mathbb{C}^2)^{\otimes 3}$ and a unitary U acting on V such that

$$U^\dagger (P A_i P^\dagger) U = X_i, \quad (51)$$

$$U^\dagger (P B_i P^\dagger) U = Z_i, \quad (52)$$

where X_i and Z_i are X and Z Pauli matrices acting on qubit i , and

$$U(P|\psi\rangle) = |G\rangle \quad (53)$$

with $|G\rangle$ being the three-qubit complete graph state defined in Eq. (11).

Proof. A quantum state $|\psi\rangle$ that belongs to a Hilbert space \mathcal{H} and a set of observables A_i, B_j acting on \mathcal{H} attain the maximal quantum violation of inequality (20) if and only if they satisfy the set of Eqs. (24)–(27). The algebraic relations induced by this set of equations let us prove Lemmas 1–3 which imply that there exists a projection $P : \mathcal{H} \rightarrow V \cong \mathbb{C}^8$ and a unitary $U = U_1(\mathbb{1}_2 \otimes U_2)(\mathbb{1}_2 \otimes \mathbb{1}_2 \otimes U_3)$ acting on $V \cong \mathbb{C}^8$ for which Eqs. (51) hold true.

From the above characterization of the observables we can infer the form of the state $|\psi\rangle$. Indeed, after plugging Eqs. (78) into the conditions (24) one realizes that the latter are simply the stabilizing conditions of the graph state associated to the complete graph of three vertices given in Eq. (11) and thus $U|\psi\rangle = |G'\rangle$. This completes the proof. ■

A few comments are in order. The first is that the tensor product structure here is just a suitable mathematical tool we used to represent our results. We know that in composite quantum systems the Hilbert space of the whole system is a tensor product of the Hilbert spaces of the separate subsystems; however, it has to be clear that in Theorem 1 we do not assume the whole system to be composite.

The second comment is that the certification statement made in Theorem 1 involves a global unitary operation which means that any state from V can in fact be chosen as the reference state, even a fully product one. Thus, Theorem 1 cannot be understood as a certification of only the state, but rather as a certification of a state and a set of measurements at the same time. Or, more precisely, it is a certification of how measurements act on the state or what the relation between a state and measurements is; this relation is basis independent.

One way to get rid of the above ambiguity is to assume that the quantum system at hand is composed of spatially separated subsystems on which the verifier can perform local measurements. Such an assumption allows them to use Bell nonlocality to deduce the form of the state. For instance for the GHZ state of three qubits a self-testing statement based on the violation of inequality (20) was derived in Ref. [17].

To illustrate the difference between contextuality and nonlocality-based certification let us consider another set of quantum observables on \mathbb{C}^8 defined as

$$\begin{aligned} A_1 &= X \otimes \mathbb{1} \otimes \mathbb{1}, & A_2 &= \mathbb{1} \otimes X \otimes Z, & A_3 &= \mathbb{1} \otimes Z \otimes X, \\ B_1 &= Z \otimes \mathbb{1} \otimes \mathbb{1}, & B_2 &= \mathbb{1} \otimes Z \otimes \mathbb{1}, & B_3 &= \mathbb{1} \otimes \mathbb{1} \otimes Z. \end{aligned} \quad (54)$$

Clearly, these observables, similarly to those in Eq. (21), satisfy the commutation and anticommutation relations in

Eqs. (22) and (30). Moreover, they give rise to the maximal violation of inequality (20) together with the graph state $|G''\rangle$ corresponding to the linear graph in Fig. 2. However, while both the graph states $|G'\rangle$ and $|G''\rangle$ are equivalent under local unitary operations and thus cannot be distinguished within both approaches to self-testing, the sets of observables in Eqs. (21) and (54) are certainly not; they are equivalent under global unitary operations. Thus, the maximal violation of the Bell inequality (20) would allow one to distinguish between these two sets, while standard quantum contextuality does not allow to do that.

IV. A SCALABLE INEQUALITY AND SELF-TESTING OF MULTIQUBIT GRAPH STATES

In this section we design a family of noncontextuality inequalities which is scalable and aimed to certify multiqubit quantum systems. These inequalities are scalable since the numbers of measurements and correlators increase polynomially with the number of vertices of the respective graph state. The inequality we propose in Eq. (57) generalizes the inequality given in Eq. (20) and has this inequality in the heart of the construction since the structure of the simplest inequality appears as the building blocks of the general construction. We prove that the inequalities are useful for certification purposes.

A. Scalable noncontextuality inequalities

First, let us consider a set of $2n$ observables denoted by A_1, \dots, A_n and B_1, \dots, B_n . They are assumed to mutually commute except for pairs A_i, B_i with $i \in \{1, \dots, n\}$, that is,

$$[A_i, A_j] = [B_i, B_j] = [A_i, B_j] = 0 \quad (i \neq j). \quad (55)$$

We now describe our construction of the noncontextuality inequalities. We first consider a sum of n expectation values of the form $C_i = \langle B_1 \cdots B_{i-1} A_i B_{i+1} \cdots B_n \rangle$ for $i = 1, \dots, n$ which involve $n-1$ different B_j observables and a single observable A_i . Then, for any choice of three out of n such different correlators C_i, C_j and C_k ($i \neq j \neq k$) we consider another correlator that we subtract from the sum. It is given by

$$\langle B_1 \cdots A_i \cdots A_j \cdots A_k \cdots B_n \rangle \quad (56)$$

and consists of three observables A_i, A_j , and A_k and $n-3$ observables B_m with $m \neq i, j, k$. In this way we obtain $n + \binom{n}{3}$ expectation values from which we construct our noncontextuality inequality,

$$\begin{aligned} \mathcal{I}_n &= \alpha_n (\langle A_1 B_2 B_3 B_4 \cdots B_n \rangle + \langle B_1 A_2 B_3 B_4 \cdots B_n \rangle + \langle B_1 B_2 A_3 B_4 \cdots B_n \rangle + \cdots + \langle B_1 B_2 B_3 B_4 \cdots A_n \rangle) \\ &\quad - \langle A_1 A_2 A_3 B_4 \cdots B_n \rangle - \langle A_1 A_2 B_3 A_4 \cdots B_n \rangle - \cdots - \langle B_1 \cdots B_{n-3} A_{n-2} A_{n-1} A_n \rangle \leq \eta_C^{(n)} < \eta_Q^{(n)} = \alpha_n n + \binom{n}{3}, \end{aligned} \quad (57)$$

where the constant $\alpha_n = \binom{n-1}{2}$ has been added for further convenience.

It is not difficult to see that for the case $n = 3$ the above inequality reproduces the one in Eq. (20). While, as already

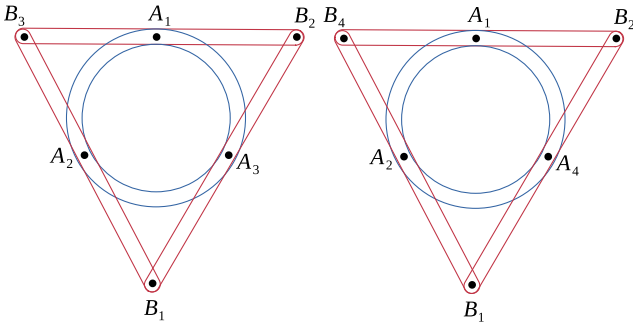


FIG. 4. Hypergraphs of compatibility of subsets of observables related with two choices of subsets of correlators in Eq. (58). On the left we have the hypergraph associated with the subscripts 1, 2, and 3, and on the right side with the subscripts 1, 2, and 4. These two hypergraphs also represent the compatibility structures of the observables corresponding to the simpler inequality (20) and another such simpler inequality with the observables A_i and B_j , with $i, j = 1, 2, 4$, respectively. These two compatibility structures serve as the building blocks to construct inequality (58).

mentioned, for $n = 3$ it is equivalent to the MABK inequality [38–40] if the commutation relations between the observables are satisfied due to the spatial separation between the subsystems, for $n > 3$ this is not the case. The number of terms in the MABK Bell-type inequalities grows exponentially with n , whereas in our noncontextuality inequalities this number scales only polynomially with n . In Refs. [18,42,50] other Bell-type inequalities were designed for the graph states which again scale exponentially or linearly; thus, they differ from our inequalities. Our inequalities (57) are designed such that they are suitable for the purpose of certification. It is also important to notice that our inequality is constructed in such a way that for every three different correlators that enter \mathcal{I}_n with $+$ and the associated “negative” one, the noncommon observables appearing in all these four correlators adopt the compatibility structure from the simplest inequality for $n = 3$. To illustrate this with an example let us consider the inequality for $n = 4$:

$$\begin{aligned} \mathcal{I}_4 = & 3(\langle A_1 B_2 B_3 B_4 \rangle + \langle B_1 A_2 B_3 B_4 \rangle + \langle B_1 B_2 A_3 B_4 \rangle \\ & + \langle B_1 B_2 B_3 A_4 \rangle) - \langle B_1 A_2 A_3 A_4 \rangle - \langle A_1 B_2 A_3 A_4 \rangle \\ & - \langle A_1 A_2 B_3 A_4 \rangle - \langle A_1 A_2 A_3 B_4 \rangle \\ \leq & \eta_C^{(4)} < \eta_Q^{(4)} = 16. \end{aligned} \quad (58)$$

Figure 4 presents the compatibility structures of the common observables for two choices of such four-element subsets of expectation values in \mathcal{I}_4 . The first subset consists of the first three terms with a $+$ sign and the last one with a $-$ sign, all containing observables A_1, A_2 , and A_3 , whereas the second set is composed of the first, the second, and the fourth “ $+$ ” terms in \mathcal{I}_4 and the third “negative one,” all of them containing A_1, A_2 , and A_4 .

Inequality (57) is nontrivial for any n , i.e., $\eta_C^{(n)} < \eta_Q^{(n)}$. To prove this statement, let us first notice that its quantum bound is $\eta_Q^{(n)} = n\alpha_n + \binom{n}{3}$ and can be attained by the following observables,

$$A_i = X_i, \quad B_j = Z_j, \quad (59)$$

and the unique graph state $|G_n\rangle$ associated to the complete graph of n qubits and stabilized by the operators in Eq. (17). In fact, plugging Eqs. (59) into the expression for \mathcal{I}_n one realizes that all correlators with $+$ correspond to the stabilizing operators G_i , whereas those entering \mathcal{I}_n with a minus sign correspond to products of triples of different G_i ’s.

Let us then estimate the maximal classical value $\eta_C^{(n)}$, and, for pedagogical purposes, we first consider the case $n = 4$ for which the expression \mathcal{I}_4 can be stated as

$$\begin{aligned} \mathcal{I}_4 = & (\langle A_1 B_2 B_3 B_4 \rangle + \langle B_1 A_2 B_3 B_4 \rangle + \langle B_1 B_2 A_3 B_4 \rangle \\ & - \langle A_1 A_2 A_3 B_4 \rangle) + (\langle A_1 B_2 B_3 B_4 \rangle + \langle B_1 A_2 B_3 B_4 \rangle \\ & + \langle B_1 B_2 B_3 A_4 \rangle - \langle A_1 A_2 B_3 A_4 \rangle) + (\langle A_1 B_2 B_3 B_4 \rangle \\ & + \langle B_1 B_2 A_3 B_4 \rangle + \langle B_1 B_2 B_3 A_4 \rangle - \langle A_1 B_2 A_3 A_4 \rangle) \\ & + (\langle B_1 A_2 B_3 B_4 \rangle + \langle B_1 B_2 A_3 B_4 \rangle + \langle B_1 B_2 B_3 A_4 \rangle \\ & - \langle B_1 A_2 A_3 A_4 \rangle), \end{aligned} \quad (60)$$

where each line in the right-hand side of the above equation corresponds to a lifting of \mathcal{I}_3 to $n = 4$. Due to the fact that in each line we have basically the inequality for $n = 3$, it is not difficult to see that for noncontextual models, $|\mathcal{I}_4| \leq 4 \times 2 = 8$, which is clearly smaller than the maximal quantum value $\eta_Q^{(4)} = 16$. To prove that the same holds true for any n , it suffices to notice that, analogously to \mathcal{I}_4 , \mathcal{I}_n can be rewritten as a sum of $\binom{n}{3}$ terms that are liftings of \mathcal{I}_3 , and thus $\eta_C^{(n)} \leq 2\binom{n}{3}$. At the same time, $\eta_Q^{(n)} = n\binom{n-1}{2} + \binom{n}{3}$ and thus $\eta_Q^{(n)} > \eta_C^{(n)}$ for any $n \geq 3$.

B. Certification based on the noncontextuality inequality

Let us now show how the above inequality can be used for certification of the complete graph state and n pairs of anti-commuting observables. To this aim, we assume that a state $|\psi\rangle \in \mathcal{H}$ together with a set of $2n$ dichotomic observables A_i and B_i acting on \mathcal{H} maximally violate Eq. (57). Then, as in the case $n = 3$, this implies the following set of $n + \binom{n}{3}$ equations:

$$B_1 \cdots B_{i-1} A_i B_{i+1} |\psi\rangle = |\psi\rangle \quad (61)$$

with $i = 1, \dots, n$, and

$$B_1 \cdots A_i \cdots A_j \cdots A_k \cdots B_n |\psi\rangle = -|\psi\rangle \quad (62)$$

for any choice of $i, j, k = 1, \dots, n$ such that $i \neq j \neq k$.

As a consequence of these equations, we have

$$A_1 B_1 |\psi\rangle = A_1 A_2 B_3 B_4 \cdots B_n |\psi\rangle = A_2 B_2 |\psi\rangle, \quad (63)$$

where the first and the second equality stem from Eq. (61) for $i = 2$ and Eq. (61) for $i = 1$, respectively. Then, by applying Eq. (62) for $i = 1, j = 2$, and $k = 3$, one obtains

$$A_1 B_1 |\psi\rangle = -B_3 A_3 |\psi\rangle. \quad (64)$$

On the other hand, using Eq. (61) with $i = 3$ we can write

$$A_1 B_1 |\psi\rangle = A_1 A_3 B_2 B_4 \cdots B_n |\psi\rangle = A_3 B_3 |\psi\rangle, \quad (65)$$

where the second equation is a consequence of Eq. (61) for $i = 1$. Simultaneously, an application of Eq. (62) for $i = 1, j = 2$, and $k = 3$ to the second terms in the above gives

$$A_1 B_1 |\psi\rangle = -B_2 A_2 |\psi\rangle. \quad (66)$$

Note that our inequality is designed in a such way that it is symmetric under any permutation of subscripts; i.e., it is invariant under the transformations $A_i \leftrightarrow A_j$ together with $B_i \leftrightarrow B_j$. This when applied to Eqs. (63)–(66) results in the following relations:

$$A_i B_j |\psi\rangle = A_j B_i |\psi\rangle = -B_i A_i |\psi\rangle \quad (67)$$

for $i, j \in \{1, 2, \dots, n\}$. In particular, A_i and B_i anticommute:

$$\{A_i, B_i\} |\psi\rangle = 0 \quad (i = 1, \dots, n). \quad (68)$$

Having established the key relations between the state and the observables, let us now, analogously to the case $n = 3$, identify a subspace of the Hilbert space \mathcal{H} which is invariant under the action of all observables A_i and B_i . The subspace is given by

$$V_n = \text{span}\{|\psi\rangle, B_{i_1} |\psi\rangle, B_{i_1} B_{i_2} |\psi\rangle, \dots, B_{i_1} B_{i_2} \dots B_{i_k} |\psi\rangle, \dots, B_{i_1} B_{i_2} \dots B_{i_{n-1}} |\psi\rangle, B_1 \dots B_n |\psi\rangle\}, \quad (69)$$

where $i_j = 1, \dots, n$ for any j and $i_1 < i_2 < \dots < i_k < \dots < i_{n-1}$.

For instance, in the simplest cases of $n = 3$ and $n = 4$, the above construction gives

$$V_3 = \text{span}\{|\psi\rangle, B_i |\psi\rangle, B_i B_j |\psi\rangle, B_1 B_2 B_3 |\psi\rangle\} \quad (70)$$

and

$$V_4 = \text{span}\{|\psi\rangle, B_i |\psi\rangle, B_i B_j |\psi\rangle, B_i B_j B_k |\psi\rangle, B_1 B_2 B_3 B_4 |\psi\rangle\} \quad (71)$$

with $i, j, k = 1, \dots, n$ and $i < j < k$. In particular, V_3 is exactly the same as the one defined in Eq. (31); due to Eq. (61), $B_i B_j |\psi\rangle = A_k |\psi\rangle$ with $i \neq j \neq k$ and $B_1 B_2 B_3 |\psi\rangle = A_1 B_1 |\psi\rangle$.

Let us then notice that the number of vectors spanning V_n is 2^n . This is because each subset of vectors of the form $A_{i_1} \dots A_{i_k} |\psi\rangle$ for $i_1 < \dots < i_k$ contains $\binom{n}{k}$ elements, and we have $n + 1$ such subsets indexed by $k = 0, \dots, n$. Thus the total number of vectors can be counted as

$$\sum_{k=0}^n \binom{n}{k} = (1 + 1)^n = 2^n, \quad (72)$$

meaning that $\dim V_n \leq 2^n$. In fact, as we show later $\dim V_n$ is exactly 2^n .

Our aim now is to identify the form of the operators A_i and B_j projected onto the subspace V_n . The idea of the proof of self-testing is similar to those we used in the case $n = 3$.

Lemma 4. The subspace V_n of \mathcal{H}_n is invariant under the action of the operators A_i and B_j for $i, j = \{1, 2, \dots, n\}$.

Proof. It can be checked that the action of any operator A_i or B_j over all the set of 2^n elements that generate the subspace V_n is, up to the factor -1 , a permutation over this set. Indeed, the action of B_m on vectors of the form $B_{i_1} \dots B_{i_k} |\psi\rangle$ with $i_1 < \dots < i_k$ for $k = 1, \dots, n$ returns vectors of a similar form with $k \rightarrow k - 1$ if m equals one of the subscripts i_1, \dots, i_k , or with $k \rightarrow k + 1$ otherwise. In both cases the resulting vectors are already in V_n .

Let us then consider the A_i observables. Due to Eq. (61) and taking into account the commutation (55) or anticommutation (68) their action on the vectors spanning V_n can always be represented as an action of a product of $n - 1$ different B_i observables. Thus, when applied to $B_{i_1} \dots B_{i_k} |\psi\rangle$

with $i_1 < \dots < i_k$ for $k = 1, \dots, n$ they will again produce vectors involving products of B_i operators that are already in V_n . This completes the proof. ■

This is a key step of our considerations because, taking into account the fact that A_i and B_i are quantum observables, Lemma 4 implies that they can be represented as a direct sum of two blocks,

$$A_i = \hat{A}_i \oplus A'_i, \quad B_j = \hat{B}_j \oplus B'_j, \quad (73)$$

where \hat{A}_i and \hat{B}_i are projections of A_i and B_i onto V_n , that is, $\hat{A}_i = P_n A_i P_n$ and $\hat{B}_i = P_n B_i P_n$ with $P_n : \mathcal{H}_n \rightarrow V_n$ denoting the projector onto V_n . On the other hand, A'_i and B'_j are defined on the orthocomplement of V_n in the Hilbert space \mathcal{H}_n that we denote V_n^\perp ; clearly, $\mathcal{H}_n = V_n \oplus V_n^\perp$.

Importantly, A'_i and B'_j act trivially on the subspace V_n , in particular $A'_i |\psi\rangle = B'_j |\psi\rangle = 0$, and consequently it is enough for our purposes to characterize \hat{A}_i and \hat{B}_j . Our first step to achieve this goal is to prove the following lemma.

Lemma 5. $\{\hat{A}_i, \hat{B}_i\} = 0$ for all $i \in \{1, \dots, n\}$.

Proof. In order to prove this statement we will show that $\{A_i, B_i\} V_n = 0$; that is, all these anticommutators act trivially on any vector from V_n . To this aim, let us investigate how $\{A_i, B_i\}$ acts on the vectors spanning V_n . We first see that $\{A_i, B_i\} |\psi\rangle = 0$ as a direct consequence of Eq. (67). Let us then consider vectors $B_j |\psi\rangle$. If $i \neq j$, we can directly use the commutation relations (55) to write

$$\{A_i, B_i\} B_j |\psi\rangle = B_j \{A_i, B_i\} |\psi\rangle = 0. \quad (74)$$

On the other hand, if $i = j$, one has

$$\{A_i, B_i\} B_i |\psi\rangle = (A_i + B_i A_i B_i) |\psi\rangle = 0, \quad (75)$$

where the last equality is again a consequence of the facts that $A_i B_i |\psi\rangle = -B_i A_i |\psi\rangle$ and that $B_i^2 = \mathbb{1}$.

It is not difficult to realize that the above reasoning extends to any vector spanning the subspace V_n . Indeed, let us consider vectors of the form $B_{i_1} \dots B_{i_k} |\psi\rangle$ with $i_1 < \dots < i_k$ for $k = 1, \dots, n$ and assume first that all i_1, \dots, i_k differ from i . Then, due to the commutation relations, one directly has

$$\{A_i, B_i\} B_{i_1} \dots B_{i_k} |\psi\rangle = B_{i_1} \dots B_{i_k} \{A_i, B_i\} |\psi\rangle = 0. \quad (76)$$

On the other hand, if one of the subscripts, say, i_1 , equals i , then

$$\begin{aligned} \{A_i, B_i\} B_{i_1} \dots B_{i_k} |\psi\rangle &= B_{i_2} \dots B_{i_k} \{A_i, B_i\} B_{i_1} |\psi\rangle \\ &= B_{i_2} \dots B_{i_k} (A_i + B_i A_i B_i) |\psi\rangle \\ &= 0, \end{aligned} \quad (77)$$

where the last equality follows from the fact that A_i and B_i anticommute when acting on $|\psi\rangle$ and from $B_i^2 = \mathbb{1}$.

Taking into account that each $\{A_i, B_i\}$ is a Hermitian operator and that it acts trivially on the whole subspace V_n , one directly concludes that $\{\hat{A}_i, \hat{B}_i\} = 0$. ■

Our next lemma is a straightforward generalization of Lemma 3.

Lemma 6. Suppose the maximal quantum violation of our inequality (57) is observed. Then, there exists a basis of V_n for which

$$\hat{A}_i = X_i, \quad \hat{B}_j = Z_j. \quad (78)$$

Proof. We will proceed recursively starting from the pair \hat{A}_1 and \hat{B}_1 . It follows from Lemma 5 that $\{\hat{A}_1, \hat{B}_1\} = 0$ which means that the dimension $d = \dim V_n$ is an even number, i.e., $d = 2k$ for some $k = 1, \dots, 2^{n-1}$ (recall that $d \leq 2^n$), and that there exists a unitary U_1 acting on V_n such that

$$U_1^\dagger \hat{A}_1 U_1 = X \otimes \mathbb{1}_k, \quad (79)$$

$$U_1^\dagger \hat{B}_1 U_1 = Z \otimes \mathbb{1}_k, \quad (80)$$

where $\mathbb{1}_k$ is an identity acting on \mathbb{C}^k .

Next, to determine the remaining observables \hat{A}_i and \hat{B}_i we exploit the fact that they all must commute with both \hat{A}_1 and \hat{B}_1 . With this aim, we use the fact that $V_n = \mathbb{C}^2 \otimes \mathbb{C}^k$ to decompose \hat{A}_i and \hat{B}_i ($i = 2, \dots, n$) in terms of the Pauli basis as

$$U_1^\dagger \hat{R}_i U_1 = \mathbb{1} \otimes M_0^R + X \otimes M_1^R + Y \otimes M_2^R + Z \otimes M_3^R, \quad (81)$$

where $R = A, B$, and M_i^R are some Hermitian matrices acting on \mathbb{C}^k . Now, $[\hat{R}_i, \hat{A}_1] = 0$ implies that $M_2^R = M_3^R = 0$, whereas from $[\hat{R}_i, \hat{B}_1] = 0$ one concludes that $M_1^R = 0$. As a result, all \hat{A}_i and \hat{B}_i with $i = 2, \dots, n$ admit the following representation,

$$U_1^\dagger \hat{A}_i U_1 = \mathbb{1}_2 \otimes M_i, \quad U_1^\dagger \hat{B}_i U_1 = \mathbb{1}_2 \otimes N_i, \quad (82)$$

where M_i and N_i act on \mathbb{C}^k ; in fact, they are Hermitian and obey $M_A^2 = M_B^2 = \mathbb{1}_k$, and thus are quantum observables. Moreover, it follows from Lemma 5 that $\{M_i, N_i\} = 0$ for all $i = 2, \dots, n$.

We have thus a set of $2(n-1)$ quantum observables M_i and N_i that satisfy the same commutation and anticommutation relations as \hat{A}_i and \hat{B}_i , and therefore we can use the above reasoning again to conclude that the dimension k is even, that is, $k = 2k'$ for some $k' = 1, \dots, 2^{n-4}$, and that there is a unitary operation $U_2 : \mathbb{C}^k \rightarrow \mathbb{C}^{k'}$ such that

$$U_2^\dagger M_2 U_2 = X \otimes \mathbb{1}_{k'}, \quad U_2^\dagger N_2 U_2 = Z \otimes \mathbb{1}_{k'}, \quad (83)$$

where $\mathbb{1}_{k'}$ is an identity acting on $\mathbb{C}^{k'}$. We then use the fact that the other operators M_i and N_i with $i = 3, \dots, n$ commute with both M_2 and N_2 to see that they are of the form $M_i = \mathbb{1}_2 \otimes P_i$ and $N_i = \mathbb{1}_2 \otimes Q_i$, where P_i and Q_i are quantum observables acting on $\mathbb{C}^{k'}$.

It is now clear that the above procedure can be applied iteratively many times until all the observables are proven to be of the form (78), of course, up to certain unitary operation. In fact, one finds that $V_n = (\mathbb{C}^2)^{\otimes n}$; that is, it is an n -qubit Hilbert space. Moreover, there is a unitary operation U composed of all the intermediate unitary operations U_i such that

$$U^\dagger \hat{A}_i U = X_i, \quad U^\dagger \hat{B}_i U = Z_i, \quad (84)$$

for any $i = 1, \dots, n$. ■

One of the main messages that one takes from this lemma is that the dimension of V_n is exactly 2^n ; in other words, V_n is isomorphic to an n -qubit Hilbert space. In this sense our inequalities can be seen as dimension witnesses: the dimension of the Hilbert space supporting a state and observables giving rise to the maximal violation of our inequalities must be at least 2^n . Moreover, the above lemma implies that a set of n pairs of anticommuting quantum observables with outcomes ± 1 that satisfy the commutation relations (55) can always

be represented, up to a single unitary operation, as a tensor product of single-qubit operators (78). We have thus arrived at our main result.

Theorem 2. If a quantum state $|\psi\rangle$ and a set of dichotomic observables A_i and B_j with $i, j = \{1, 2, \dots, n\}$ give rise to maximal violation of inequality (57), then there exist a projection $P_n : \mathcal{H}_n \rightarrow \mathbb{C}^{2^n}$ and a unitary U acting on \mathbb{C}^{2^n} such that

$$U^\dagger (P A_i P^\dagger) U = \hat{A}_i, \quad (85)$$

$$U^\dagger (P B_j P^\dagger) U = \hat{B}_j, \quad (86)$$

$$U(P|\psi\rangle) = |G_n\rangle, \quad (87)$$

where \hat{A}_i and \hat{B}_j are defined in Eq. (78) and $|G_n\rangle$ is the complete graph state of n qubits.

Proof. The state $|\psi\rangle \in \mathcal{H}_n$ and observables A_i and B_j acting on the Hilbert space \mathcal{H}_n attain the maximal quantum violation of inequality (57) if, and only if, they satisfy the set of $n + \binom{n}{3}$ equations (61) and (62). The algebra induced by this set of equations allows us to prove Lemmas 4, 5, and 6; in particular, it follows that there exists a projection $P_n : \mathcal{H} \rightarrow V_n \cong \mathbb{C}^{2^n}$ and a unitary U acting on V_n such that

$$U^\dagger (P A_i P^\dagger) U = X_i, \quad (88)$$

$$U^\dagger (P B_j P^\dagger) U = Z_j. \quad (89)$$

In this way, the products of observables that appear in the first n correlators in inequality (57) give stabilizing operators of the graph state associated to the complete graph with n vertices, whereas the correlators with negative sign correspond to products of three different stabilizing operators for which the graph state $|G_n\rangle$ is an eigenvector with associated eigenvalue -1 . Thus the complete graph state will be the unique state that attains the maximal quantum violation; then

$$U(P|\psi\rangle) = |G_n\rangle. \quad (90)$$

This completes the proof. ■

V. ROBUSTNESS

Here we obtain fidelity bounds on the state and measurements leading to the given nonmaximal violation of inequality (57) to demonstrate that our scheme is robust to errors and experimental imperfections. For simplicity, let us focus on the case of $n = 3$. Let us say that the maximal quantum violation of inequality (20) is observed with an ϵ error, i.e., a non-maximal violation of $4 - \epsilon$ is observed. Then, the correlators satisfy the following bounds:

$$\begin{aligned} \langle \psi | A_1 B_2 B_3 | \psi \rangle &\geq 1 - \epsilon, \\ \langle \psi | B_1 A_2 B_3 | \psi \rangle &\geq 1 - \epsilon, \\ \langle \psi | B_1 B_2 A_3 | \psi \rangle &\geq 1 - \epsilon, \\ -\langle \psi | A_1 A_2 A_3 | \psi \rangle &\geq 1 - \epsilon, \end{aligned} \quad (91)$$

for some $\epsilon > 0$. We demonstrate that for a small enough value of ϵ , the quantum realization is close enough to the optimal quantum realization which leads to the maximal quantum violation of the inequality. This is the purpose of robustness analysis that will be presented here; i.e., we show that in the

limit $\epsilon \rightarrow 0$ the quantum realization is close to the optimal one.

In the presence of errors, it is not straightforward to guarantee the existence of an invariant subspace under the action of the operators A_i and B_j , as we have in the self-testing of the optimal quantum realization. However, the robustness of the protocol can be demonstrated, in a similar way to that of Ref. [32], by proving the existence of an eight-dimensional ideal subspace \hat{V} together with a state $|\hat{\psi}\rangle \in \hat{V}$ and observables \hat{A}_i and \hat{B}_i acting on it such that their fidelities with the actual state and measurements approach one in the limit of $\epsilon \rightarrow 0$. We define the state fidelity as $F(|\hat{\psi}\rangle, |\psi\rangle) := |\langle \hat{\psi} | \psi \rangle|^2$, and the operator fidelity as $F(\hat{X}_i, X_i) := (1/8)\text{Tr}(\hat{X}_i X_i)$ (with $X_i = A_i$), where the $1/8$ factor is used to normalize the fidelity since $\text{Tr}(\hat{X}_i X_i) \leq 8$, and similarly defined between \hat{B}_j and B_j . Formally, we have the following theorem.

Theorem 3. Suppose a quantum state $|\psi\rangle$ and a set of measurements A_i, B_j with $i, j = \{1, 2, 3\}$ in a Hilbert space \mathcal{H} satisfy the ideal expectations corresponding to the maximal quantum violation of inequality (20) to within error ϵ . Then there exists a projection $P : \mathcal{H} \rightarrow \hat{V}$, where $\dim(\hat{V}) = 8$, a state $|\hat{\psi}\rangle \in \hat{V}$ and \hat{A}_i, \hat{B}_j which are Hermitian involutions acting on \hat{V} for all i and j such that

$$\begin{aligned} \langle \hat{\psi} | \hat{A}_1 \hat{B}_2 \hat{B}_3 | \hat{\psi} \rangle &= 1, \\ \langle \hat{\psi} | \hat{B}_1 \hat{A}_2 \hat{B}_3 | \hat{\psi} \rangle &= 1, \\ \langle \hat{\psi} | \hat{B}_1 \hat{B}_2 \hat{A}_3 | \hat{\psi} \rangle &= 1, \end{aligned}$$

and there exists some unitary U acting on \hat{V} such that

$$\begin{aligned} F(U|\hat{\psi}\rangle, |\psi\rangle) &\geq 1 - \epsilon_0, \\ F(U\hat{A}_i U^\dagger, A_i) &\geq 1 - \epsilon_1 \quad \forall i, \\ F(U\hat{B}_j U^\dagger, B_j) &\geq 1 - \epsilon_2 \quad \forall j, \end{aligned}$$

where $\epsilon_0 = 25\epsilon$, $\epsilon_1 = 0$, and $\epsilon_2 = 4\epsilon$.

The proof of the above theorem is given in Appendix A. This theorem implies that there exists a subspace in which, up to a small enough error, the quantum realization leading to the nonmaximal quantum violation is close to the optimal quantum realization up to a unitary. For instance, an error of 0.1% in each expectation value implies that the state fidelity is not less than 97.5% and the operator fidelities of B_j are not less than 99.6%. Following the proof of Theorem 3, one can also obtain the fidelity bounds for any n demonstrating the robustness of the scheme similarly as presented in Theorem 4.

In order to obtain a tight self-testing bound that is applicable to a more noisy practical scenario in which the given nonmaximal violation is not almost perfect, one may employ the numerical method to bound the state fidelity as a function of violation of the noncontextual inequality based on semidefinite programming relaxations of quantum contextual sets introduced in Ref. [51] or the analytical method based on operator inequalities introduced in Ref. [17].

VI. CONCLUSIONS

Quantum contextuality provides a notion of nonclassicality for single systems. Motivated by extending the task of self-testing based on Bell inequalities to scenarios where en-

tanglement is not necessary or spatial separation between the subsystems is not required, self-testing of quantum devices based on quantum contextuality has recently been explored. In this work we have followed this research direction and have introduced a family of inequalities revealing quantum contextuality and have shown that they can be used for certification of multiqubit quantum systems. An interesting feature of our scheme is that it is scalable: the amount of information about the observed nonclassical correlations needed to certify the underlying quantum system grows only polynomially with the number of qubits that are certified.

Such contextuality-based certification schemes rely, however, on compatibility relations between the involved measurements and are thus generally difficult to implement in practice. A natural follow-up of this work would be therefore to design a scheme for certification built on our inequalities that does not rely on the compatibility relations, but rather allows one to deduce them from the observed nonclassicality. Such schemes for single quantum systems have recently been proposed in Refs. [33,34] within the sequential measurements or temporal correlations scenario. It would be thus interesting to see whether our results can be mapped to this scenario. Another possible direction for further research is to explore whether one can improve the scalability of our scheme with the number of the certified qubits. From a general perspective it is a highly nontrivial question to ask what is the minimal information about the observed nonclassical correlations that enables making nontrivial statements about the underlying quantum system.

ACKNOWLEDGMENTS

We thank D. Saha for discussions. We are also indebted to O. Makuta for providing us the example presented at the end of Sec. III. This work was supported by the Foundation for Polish Science through the First Team project (First TEAM/2017-4/31) co-financed by the European Union under the European Regional Development Fund.

APPENDIX A: PROOF OF THEOREM 3

Here we present the derivation of robustness of the scheme given in Theorem 3. This will be similar to the proof of robustness of the certification scheme given in Ref. [32].

For providing robust self-testing statements in the Bell tests where dichotomic measurements are implemented [17], Jordan decomposition for the state and measurements has been employed to simplify the derivation. In Ref. [32], Jordan decomposition has also been extended to the contextuality scenario to provide robust certification of the two-qubit system. In Appendix B, we extend this Jordan decomposition to our scenario to provide the robust certification. According to this decomposition, we can decompose the Hilbert space \mathcal{H} in which the state and measurements leading to the violation of our inequality act as

$$\mathcal{H} = \bigoplus_l \mathcal{H}_l, \quad (\text{A1})$$

where each \mathcal{H}_l has dimension at most eight and is invariant under the action of A_i and B_j .

With respect to decomposition (A1), the state $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_l \sqrt{p_l} |\psi_l\rangle, \quad (\text{A2})$$

where $|\psi_l\rangle \in \mathcal{H}_l$ and $\sum_l p_l = 1$. We express each $|\psi_l\rangle$ in the computational basis $\{|abc\rangle_l : a, b, c \in \{0, 1\}\}$ as

$$|\psi_l\rangle = \sum_{a,b,c=0,1} c_{abc}^{(l)} |abc\rangle_l, \quad (\text{A3})$$

where $c_{abc}^{(l)}$ satisfies $\sum_{a,b,c} |c_{abc}^{(l)}|^2 = 1$.

We define the subspace $\hat{V} \subseteq \mathcal{H}$ as the linear span of $\{|\tilde{a}\tilde{b}\tilde{c}\rangle := \sum_l \sqrt{p_l} |abc\rangle_l\}$. We define the ideal state in this subspace as

$$|\hat{\psi}\rangle := \frac{1}{\sqrt{2}}(|\tilde{0}\tilde{0}\tilde{0}\rangle - |\tilde{1}\tilde{1}\tilde{1}\rangle), \quad (\text{A4})$$

which can be reexpressed as

$$|\hat{\psi}\rangle = \sum_l \sqrt{p_l} |\hat{\psi}_l\rangle, \quad (\text{A5})$$

where

$$|\hat{\psi}_l\rangle := \frac{1}{\sqrt{2}}(|000\rangle_l - |111\rangle_l). \quad (\text{A6})$$

Note that for the ideal observables defined as

$$\begin{aligned} \hat{A}_1 &:= \bigoplus_l (\hat{A}_{1_l} \otimes \mathbb{1}_l \otimes \mathbb{1}_l), & \hat{B}_1 &:= \bigoplus_l (\hat{B}_{1_l} \otimes \mathbb{1}_l \otimes \mathbb{1}_l), \\ \hat{A}_2 &:= \bigoplus_l (\mathbb{1}_l \otimes \hat{A}_{2_l} \otimes \mathbb{1}_l), & \hat{B}_2 &:= \bigoplus_l (\mathbb{1}_l \otimes \hat{B}_{2_l} \otimes \mathbb{1}_l), \\ \hat{A}_3 &:= \bigoplus_l (\mathbb{1}_l \otimes \mathbb{1}_l \otimes \hat{A}_{3_l}), & \hat{B}_3 &:= \bigoplus_l (\mathbb{1}_l \otimes \mathbb{1}_l \otimes \hat{B}_{3_l}), \end{aligned}$$

where

$$\hat{A}_{i_l} = X_i, \quad \hat{B}_{j_l} = Y_j, \quad (\text{A7})$$

where X_i and Y_j are the Pauli operators acting on the i th qubit, the ideal state defined in Eq. (A4) violates the noncontextuality inequality (20) maximally. Note that the ideal state projected onto \mathcal{H}_l , i.e., $|\hat{\psi}_l\rangle$, has the form of the GHZ state (16). We have chosen the above particular form of the ideal state for our convenience.

We now express the nonideal observables with respect to the Jordan decomposition. Due to the fact that we have three pairs of dichotomic observables that do not commute on the quantum state, which is a consequence of Lemma 7, the dimension of each of the subspaces \mathcal{H}_l in Eq. (A1) can be taken to be eight. From Corollary 1, it follows that

$$\begin{aligned} A_1 &= \bigoplus_l (A_{1_l} \otimes \mathbb{1}_l \otimes \mathbb{1}_l), & B_1 &= \bigoplus_l (B_{1_l} \otimes \mathbb{1}_l \otimes \mathbb{1}_l), \\ A_2 &= \bigoplus_l (\mathbb{1}_l \otimes A_{2_l} \otimes \mathbb{1}_l), & B_2 &= \bigoplus_l (\mathbb{1}_l \otimes B_{2_l} \otimes \mathbb{1}_l), \\ A_3 &= \bigoplus_l (\mathbb{1}_l \otimes \mathbb{1}_l \otimes A_{3_l}), & B_3 &= \bigoplus_l (\mathbb{1}_l \otimes \mathbb{1}_l \otimes B_{3_l}), \end{aligned}$$

where by using “local” unitary operations we can always choose A_{i_l} and B_{i_l} acting on \mathcal{H}_l to be other following forms:

$$\begin{aligned} A_{1_l} &= X_1, & B_{1_l} &= \cos \theta_l Y_1 + \sin \theta_l X_1, \\ A_{2_l} &= X_2, & B_{2_l} &= \cos \phi_l Y_2 + \sin \phi_l X_2, \\ A_{3_l} &= X_3, & B_{3_l} &= \cos \nu_l Y_3 + \sin \nu_l X_3, \end{aligned} \quad (\text{A8})$$

with $\theta_l, \phi_l, \nu_l \in [-\frac{\pi}{2}, \frac{\pi}{2}]$.

We now proceed to calculate the state fidelity given by $|\langle \hat{\psi} | \psi \rangle|^2$, where $|\hat{\psi}\rangle$ is the ideal state given by Eq. (A4). Using the fact that the global phase on each subspace can be chosen freely, we can always set $\langle \hat{\psi}_l | \psi_l \rangle \geq 0$, and therefore,

$$\langle \hat{\psi} | \psi \rangle = \sum_l p_l \langle \hat{\psi}_l | \psi_l \rangle \geq \sum_l p_l |\langle \hat{\psi}_l | \psi_l \rangle|^2. \quad (\text{A9})$$

Now, using the expressions of $|\psi_l\rangle$ and $|\hat{\psi}_l\rangle$ given by Eqs. (A3) and (A6), respectively, $\sum_l p_l |\langle \hat{\psi}_l | \psi_l \rangle|^2$ can be written as

$$\sum_l p_l |\langle \hat{\psi}_l | \psi_l \rangle|^2 = \sum_l p_l \frac{1}{2} |c_{000}^{(l)} - c_{111}^{(l)}|^2.$$

The expression in the right-hand side of the above equation can be written as

$$\frac{1}{2} |c_{000}^{(l)} - c_{111}^{(l)}|^2 = |c_{000}^{(l)}|^2 + |c_{111}^{(l)}|^2 - \frac{1}{2} |c_{000}^{(l)} + c_{111}^{(l)}|^2.$$

Using $\sum_{abc} |c_{abc}^{(l)}|^2 = 1$ in the first term in the right-hand side of the above equation, we arrive at

$$\begin{aligned} \sum_l p_l |\langle \hat{\psi}_l | \psi_l \rangle|^2 &= 1 - \sum_l p_l \sum_{abc \neq 000, 111} |c_{abc}^{(l)}|^2 \\ &\quad - \sum_l p_l \frac{1}{2} |c_{000}^{(l)} + c_{111}^{(l)}|^2. \end{aligned} \quad (\text{A10})$$

We will use the following lemma to obtain a lower bound on the right-hand side of the above equation.

Lemma 7. Suppose that inequalities (91) are satisfied for some $\epsilon > 0$. Then, $\|A_i, B_i\| \leq 4\sqrt{2\epsilon}$ for all i .

Proof. We show that $\|A_1, B_1\| \leq 4\sqrt{2\epsilon}$. From Eqs. (91) and assuming that $0 \leq \epsilon \leq 1$, we have that

$$\begin{aligned} \|A_1|\psi\rangle + A_2A_3|\psi\rangle\| &= \sqrt{2(1 + \langle \psi | A_1A_2A_3 | \psi \rangle)} \\ &\leq \sqrt{2[1 - (1 - \epsilon)]} \\ &= \sqrt{2\epsilon}, \end{aligned} \quad (\text{A11})$$

and, similarly, we have

$$\|B_2|\psi\rangle - B_1A_3|\psi\rangle\| \leq \sqrt{2\epsilon}, \quad (\text{A12})$$

$$\|B_1|\psi\rangle - A_2B_3|\psi\rangle\| \leq \sqrt{2\epsilon}, \quad (\text{A13})$$

$$\|B_2|\psi\rangle - A_1B_3|\psi\rangle\| \leq \sqrt{2\epsilon}. \quad (\text{A14})$$

Using then the triangle inequality for the vector norm and the fact that it is unitarily invariant, we have

$$\begin{aligned} \|(A_1B_1 + B_1A_1)|\psi\rangle\| &\leq \|(B_1A_1 + B_1A_2A_3)|\psi\rangle\| \\ &\quad + \|(-B_1A_2A_3 + A_2B_2)|\psi\rangle\| \\ &\quad + \|(-A_2B_2 + A_1A_2B_3)|\psi\rangle\| \\ &\quad + \|(-A_1A_2B_3 + A_1B_1)|\psi\rangle\| \\ &\leq 4\sqrt{2\epsilon}. \end{aligned} \quad (\text{A15})$$

Due to the symmetry of the inequality, the same will hold for any other i , which completes the proof. ■

First, let us bound $\sum_l p_l |c_{000}^{(l)} + c_{111}^{(l)}|^2$ in Eq. (A10). From Eqs. (A11) and (A12), respectively, we obtain

$$\begin{aligned} & \sum_l p_l (|c_{000}^{(l)} + c_{111}^{(l)}|^2 + |c_{001}^{(l)} + c_{110}^{(l)}|^2 \\ & \quad + |c_{010}^{(l)} + c_{101}^{(l)}|^2 + |c_{011}^{(l)} + c_{100}^{(l)}|^2) \leq \epsilon, \\ & \sum_l p_l (|e^{-i\phi_l} c_{000}^{(l)} - e^{i\theta_l} c_{111}^{(l)}|^2 + |e^{i\phi_l} c_{010}^{(l)} + e^{i\theta_l} c_{101}^{(l)}|^2 \\ & \quad + |e^{-i\phi_l} c_{001}^{(l)} - e^{i\theta_l} c_{110}^{(l)}|^2 + |e^{i\phi_l} c_{011}^{(l)} + e^{i\theta_l} c_{100}^{(l)}|^2) \leq \epsilon. \end{aligned}$$

From the first of these equations, it follows that

$$\sum_l p_l |c_{000}^{(l)} + c_{111}^{(l)}|^2 \leq \epsilon. \quad (\text{A16})$$

It also follows that

$$\sum_l p_l |c_{001}^{(l)} + c_{110}^{(l)}|^2 \leq \epsilon, \quad (\text{A17})$$

$$\sum_l p_l |e^{-i\phi_l} c_{001}^{(l)} - e^{i\theta_l} c_{110}^{(l)}|^2 \leq \epsilon. \quad (\text{A18})$$

Next, we proceed to bound $\sum_l p_l \sum_{abc \neq 000, 111} |c_{abc}^{(l)}|^2$ in Eq. (A10). We have

$$\begin{aligned} & |c_{110}^{(l)}|^2 |e^{i\theta_l} + e^{-i\phi_l}|^2 \\ & = |(e^{i\theta_l} c_{110}^{(l)} - e^{-i\phi_l} c_{001}^{(l)}) + e^{-i\phi_l} (c_{001}^{(l)} + c_{110}^{(l)})|^2. \end{aligned}$$

Using the fact that $|x + y|^2 \leq 2(|x|^2 + |y|^2)$ for any $x, y \in \mathbb{C}$ in the above equation, we arrive at

$$\begin{aligned} & |c_{110}^{(l)}|^2 |e^{i\theta_l} + e^{-i\phi_l}|^2 \\ & \leq 2(|e^{i\theta_l} c_{110}^{(l)} - e^{-i\phi_l} c_{001}^{(l)}|^2 + |c_{001}^{(l)} + c_{110}^{(l)}|^2). \end{aligned}$$

From Eqs. (A17) and (A18),

$$\begin{aligned} & \sum_l p_l |c_{110}^{(l)}|^2 |e^{i\theta_l} + e^{-i\phi_l}|^2 \\ & = \sum_l p_l |c_{110}^{(l)}|^2 (2 + 2 \cos(\theta_l + \phi_l)) \leq 4\epsilon. \end{aligned} \quad (\text{A19})$$

Similarly,

$$\begin{aligned} & |c_{001}^{(l)}|^2 |e^{i\theta_l} + e^{-i\phi_l}|^2 \\ & = |(-e^{i\theta_l} c_{110}^{(l)} + e^{-i\phi_l} c_{001}^{(l)}) + e^{i\theta_l} (c_{001}^{(l)} + c_{110}^{(l)})|^2 \\ & \leq 2(|-e^{i\theta_l} c_{110}^{(l)} + e^{-i\phi_l} c_{001}^{(l)}|^2 + |c_{001}^{(l)} + c_{110}^{(l)}|^2), \end{aligned}$$

from which it follows that

$$\begin{aligned} & \sum_l p_l |c_{001}^{(l)}|^2 |e^{i\theta_l} + e^{-i\phi_l}|^2 \\ & = \sum_l p_l |c_{001}^{(l)}|^2 (2 + 2 \cos(\theta_l + \phi_l)) \leq 4\epsilon. \end{aligned} \quad (\text{A20})$$

Adding Eqs. (A19) and (A20),

$$\sum_l p_l (|c_{001}^{(l)}|^2 + |c_{110}^{(l)}|^2) (1 + \cos(\theta_l + \phi_l)) \leq 4\epsilon. \quad (\text{A21})$$

We now need the following lemma, which is similar to Lemma 7.

Lemma 8. Suppose the ideal expectations are satisfied to within error ϵ . Then $\|A_1 B_2 |\psi\rangle + B_1 A_2 |\psi\rangle\| \leq 2\sqrt{2}\epsilon$.

Proof.

$$\begin{aligned} & \|A_1 B_2 |\psi\rangle + B_1 A_2 |\psi\rangle\| \leq \|(A_1 B_2 - A_1 B_1 A_3) |\psi\rangle\| \\ & \quad + \|(A_1 B_1 A_3 + B_1 A_2) |\psi\rangle\| \leq 2\sqrt{2}\epsilon, \end{aligned}$$

where the last inequality follows from Eqs. (A11) and (A12). ■

From the result of the lemma, we obtain

$$\begin{aligned} & \sum_l p_l (|c_{001}^{(l)}|^2 + |c_{110}^{(l)}|^2) |e^{i\theta_l} + e^{i\phi_l}|^2 \\ & \quad + (|c_{011}^{(l)}|^2 + |c_{100}^{(l)}|^2) |e^{i\theta_l} - e^{-i\phi_l}|^2 \\ & \quad + \sum_l p_l (|c_{000}^{(l)}|^2 + |c_{111}^{(l)}|^2) |e^{-i\theta_l} + e^{-i\phi_l}|^2 \\ & \quad + (|c_{010}^{(l)}|^2 + |c_{101}^{(l)}|^2) |e^{-i\theta_l} - e^{i\phi_l}|^2 \leq 8\epsilon, \end{aligned}$$

and therefore,

$$\sum_l p_l (|c_{001}^{(l)}|^2 + |c_{110}^{(l)}|^2) |e^{i\theta_l} + e^{i\phi_l}|^2 \leq 8\epsilon,$$

or

$$\sum_l p_l (|c_{001}^{(l)}|^2 + |c_{110}^{(l)}|^2) (1 + \cos(\theta_l - \phi_l)) \leq 4\epsilon. \quad (\text{A22})$$

Adding Eqs. (A21) and (A22),

$$\begin{aligned} & \frac{8}{2}\epsilon \geq \sum_l p_l (|c_{001}^{(l)}|^2 + |c_{110}^{(l)}|^2) (1 + \cos \theta_l \cos \phi_l) \\ & \geq \sum_l p_l (|c_{001}^{(l)}|^2 + |c_{110}^{(l)}|^2), \end{aligned} \quad (\text{A23})$$

where in the last inequality we used $\theta_l, \phi_l \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, and so $\cos \theta_l \geq 0$ and $\cos \phi_l \geq 0$. Similarly, from Eqs. (A13) and (A14), we have found the following bounds on $\sum_l p_l (|c_{010}^{(l)}|^2 + |c_{101}^{(l)}|^2)$ and $\sum_l p_l (|c_{011}^{(l)}|^2 + |c_{100}^{(l)}|^2)$:

$$\frac{8}{2}\epsilon \geq \sum_l p_l (|c_{010}^{(l)}|^2 + |c_{101}^{(l)}|^2), \quad (\text{A24})$$

$$\frac{8}{2}\epsilon \geq \sum_l p_l (|c_{011}^{(l)}|^2 + |c_{100}^{(l)}|^2), \quad (\text{A25})$$

respectively. Summing Eqs. (A23)–(A25), we obtain

$$\sum_l p_l \sum_{abc \neq 000, 111} |c_{abc}^{(l)}|^2 \leq \frac{24}{2}\epsilon. \quad (\text{A26})$$

Substituting Eqs. (A26) and (A16) in Eq. (A10), we obtain the state fidelity as

$$\begin{aligned} F(|\hat{\psi}\rangle, |\psi\rangle) & \geq \left(1 - \frac{25}{2}\epsilon\right)^2 \\ & \geq 1 - 25\epsilon. \end{aligned} \quad (\text{A27})$$

Next we bound the fidelity of the operators. From Eq. (A8) and the definition of the ideal operators (up to a unitary freedom), it follows that for all i , $\text{tr}(\hat{A}_i A_i) = 8$ which implies that

$F(\hat{A}_i, A_i) = 1$. From Eq. (A8), it also follows that

$$F(\hat{B}_1, B_1) = \sum_l p_l \cos \theta_l. \quad (\text{A28})$$

Let us now obtain a lower bound on $\sum_l p_l \cos \theta_l$. Using both the result of Lemma 7 and Eq. (A8), we obtain

$$\begin{aligned} 4\epsilon &\geq \frac{1}{8} \|\{A_1, B_1\}|\psi\rangle\|^2 \\ &= \sum_l p_l \sin^2 \theta_l. \end{aligned} \quad (\text{A29})$$

Using $\cos^2 \theta_l + \sin^2 \theta_l = 1$ and $\sum_l p_l = 1$, we can write $\sum_l p_l \sin^2 \theta_l$ as

$$\begin{aligned} \sum_l p_l \sin^2 \theta_l &= 1 - \sum_l p_l \cos^2 \theta_l \\ &\geq 1 - \sum_l p_l \cos \theta_l, \end{aligned} \quad (\text{A30})$$

where the inequality follows from $\theta_l \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ and therefore $\cos \theta_l \geq 0$. From the above two equations, it follows that

$$1 - \sum_l p_l \cos \theta_l \leq 4\epsilon. \quad (\text{A31})$$

Using the above equation in Eq. (A28), we obtain

$$F(\hat{B}_1, B_1) \geq 1 - 4\epsilon.$$

This ends the proof of Theorem 3.

Theorem 3 can be straightforwardly extended to any n as follows. Here the state fidelity is defined as earlier and the operator fidelity is defined with the different normalization factor as $F(\hat{X}_i, X_i) := (1/\dim(\hat{V}_n))\text{Tr}(\hat{X}_i X_i)$, where $\dim(\hat{V}_n)$ is the dimension of the invariant subspace.

Theorem 4. If a quantum state $|\psi\rangle$ and a set of measurements A_i, B_j with $i, j = \{1, 2, \dots, n\}$ in a Hilbert space \mathcal{H}_n satisfy the ideal expectations corresponding to the maximal quantum violation of inequality (57) to within error ϵ , then there exists a projection $P: \mathcal{H}_n \rightarrow \hat{V}_n$, where $\dim(\hat{V}_n) = 2^n$, a state $|\hat{\psi}\rangle \in \hat{V}_n$, and \hat{A}_i, \hat{B}_j which are Hermitian involutions acting on \hat{V}_n for all i and j such that

$$\begin{aligned} \langle \hat{\psi} | \hat{A}_1 \hat{B}_2 \hat{B}_3 \hat{B}_4 \cdots \hat{B}_n | \hat{\psi} \rangle &= 1, \\ \langle \hat{\psi} | \hat{B}_1 \hat{A}_2 \hat{B}_3 \hat{B}_4 \cdots \hat{B}_n | \hat{\psi} \rangle &= 1, \\ &\vdots \\ \langle \hat{\psi} | \hat{B}_1 \hat{B}_2 \hat{B}_3 \hat{B}_4 \cdots \hat{A}_n | \hat{\psi} \rangle &= 1, \end{aligned}$$

and there also exists a unitary U acting on \hat{V} such that

$$\begin{aligned} F(U|\hat{\psi}\rangle, |\psi\rangle) &\geq 1 - \epsilon_0, \\ F(U\hat{A}_i U^\dagger, A_i) &\geq 1 - \epsilon_1 \quad \forall i, \\ F(U\hat{B}_i U^\dagger, B_i) &\geq 1 - \epsilon_2 \quad \forall i, \end{aligned}$$

where $\epsilon_0 = [8(2^{n-1} - 1) + 1]\epsilon$, $\epsilon_1 = 0$, and $\epsilon_2 = 2^{5-n}\epsilon$.

Proof. The bounds of this theorem are obtained using the similar steps used in the proof of Theorem 3. With respect to the Jordan decomposition,

$$\mathcal{H}_n = \bigoplus_l \mathcal{H}_l, \quad (\text{A32})$$

where each \mathcal{H}_l has dimension at most 2^n and is invariant under the action of A_i and B_j . As before, the state $|\psi\rangle$ can be decomposed as

$$|\psi\rangle = \sum_l \sqrt{p_l} |\psi_l\rangle, \quad (\text{A33})$$

where $|\psi_l\rangle \in \mathcal{H}_l$ and $\sum_l p_l = 1$. With respect to the computational basis $\{|n_1 n_2 \cdots n_n\rangle_l : n_i \in \{0, 1\}\}$, we express each $|\psi_l\rangle$ as

$$|\psi_l\rangle = \sum_{n_i \in \{0, 1\}} c_{n_1 n_2 \cdots n_n}^{(l)} |n_1 n_2 \cdots n_n\rangle_l,$$

where $\sum_{n_1 n_2 \cdots n_n} |c_{n_1 n_2 \cdots n_n}^{(l)}|^2 = 1$.

We define the subspace $\hat{V}_n \subseteq \mathcal{H}_n$ as the linear span of $\{|\tilde{n}_1 \tilde{n}_2 \cdots \tilde{n}_n\rangle := \sum_l \sqrt{p_l} |n_1 n_2 \cdots n_n\rangle_l\}$. We define the ideal state in this subspace as

$$|\hat{\psi}\rangle := \frac{1}{\sqrt{2}} (|\tilde{0}_1 \tilde{0}_2 \cdots \tilde{0}_n\rangle - |\tilde{1}_1 \tilde{1}_2 \cdots \tilde{1}_n\rangle), \quad (\text{A34})$$

which can be reexpressed as

$$|\hat{\psi}\rangle = \sum_l \sqrt{p_l} |\hat{\psi}_l\rangle, \quad (\text{A35})$$

where

$$|\hat{\psi}_l\rangle := \frac{1}{\sqrt{2}} (|0_1 0_2 \cdots 0_n\rangle_l - |1_1 1_2 \cdots 1_n\rangle_l). \quad (\text{A36})$$

Note that for the ideal observables defined as

$$\begin{aligned} \hat{A}_i &:= \bigoplus_l \left(\bigotimes_{i=1}^{k-1} \mathbb{1}_l \otimes \hat{A}_i^l \otimes \bigotimes_{i=k+1}^n \mathbb{1}_l \right), \\ \hat{B}_j &:= \bigoplus_l \left(\bigotimes_{i=1}^{k-1} \mathbb{1}_l \otimes \hat{B}_j^l \otimes \bigotimes_{i=k+1}^n \mathbb{1}_l \right), \end{aligned}$$

where

$$\hat{A}_{i_l} = X_i, \quad \hat{B}_{j_l} = Y_j,$$

with $i, j = 1, 2, 3$, and, for $i, j = 4, 5, \dots, n$,

$$\hat{A}_{i_l} = -Y_i, \quad \hat{B}_{j_l} = X_j,$$

the ideal state defined in Eq. (A34) violates the noncontextuality inequality (20) maximally.

From Appendix B, it follows that the nonideal observables can be written as

$$\begin{aligned} A_i &= \bigoplus_l \left(\bigotimes_{i=1}^{k-1} \mathbb{1}_l \otimes A_i^l \otimes \bigotimes_{i=k+1}^n \mathbb{1}_l \right), \\ B_j &= \bigoplus_l \left(\bigotimes_{j=1}^{k-1} \mathbb{1}_l \otimes B_j^l \otimes \bigotimes_{j=k+1}^n \mathbb{1}_l \right), \end{aligned}$$

for all $i, j = 1, 2, \dots, n$. We choose a unitary such that the operators A_{i_l} and B_{j_l} acting on \mathcal{H}_l can be written as follows:

$$A_{i_l} = X_j, \quad B_{j_l} = \cos \theta_{ji} Y_j + \sin \theta_{ji} X_j, \quad i, j = 1, 2, 3, \quad (\text{A37})$$

$$B_{i_l} = X_k, \quad A_{j_l} = \cos \theta_{ji} Y_k + \sin \theta_{ji} X_k, \quad i, j = 4, 5, \dots, n, \quad (\text{A38})$$

with $\theta_{ji} \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ for all j and k .

Using the similar steps used to obtain Eq. (A10), we have

$$\langle \hat{\psi} | \psi \rangle \geq 1 - \sum_l p_l \sum_{n_1 n_2 \dots n_n \neq 0_1 0_2 \dots 0_n, 1_1 1_2 \dots 1_n} |c_{n_1 n_2 \dots n_n}^{(l)}|^2 - \frac{1}{2} \sum_l p_l |c_{0_1 0_2 \dots 0_n}^{(l)} + c_{1_1 1_2 \dots 1_n}^{(l)}|^2. \quad (\text{A39})$$

Similarly to the case of $n = 3$, a bound on the right-hand side of the above equation can be obtained as follows. The term $\frac{1}{2} \sum_l p_l |c_{0_1 0_2 \dots 0_n}^{(l)} + c_{1_1 1_2 \dots 1_n}^{(l)}|^2$ in Eq. (A39) can be bounded using the inequality given by

$$\|A_1 |\psi\rangle + A_2 A_3 B_4 \dots B_n |\psi\rangle\| \leq \sqrt{2\epsilon}. \quad (\text{A40})$$

From this equation, we obtain

$$\sum_l p_l (|c_{0_1 0_2 0_3 \dots 0_n}^{(l)} + c_{1_1 1_2 1_3 \dots 1_n}^{(l)}|^2 + \dots + |c_{0_1 1_2 1_3 \dots 1_n}^{(l)} + c_{1_1 0_2 0_3 \dots 0_n}^{(l)}|^2) \leq \epsilon, \quad (\text{A41})$$

from which it follows that

$$\sum_l p_l |c_{0_1 0_2 \dots 0_n}^{(l)} + c_{1_1 1_2 \dots 1_n}^{(l)}|^2 \leq \epsilon. \quad (\text{A42})$$

Next, the second term in Eq. (A39) can be bounded using the other inequalities such as

$$\|B_2 |\psi\rangle - B_1 A_3 B_4 \dots B_n |\psi\rangle\| \leq \sqrt{2\epsilon}, \quad (\text{A43})$$

from which we obtain

$$\begin{aligned} \sum_l p_l & \left(\sum_{n_4, \dots, n_n} |e^{-i\theta_{2l}} c_{000n_4 \dots n_n}^{(l)} - e^{i\theta_{1l}} c_{111\bar{n}_4 \dots \bar{n}_n}^{(l)}|^2 \right. \\ & + \sum_{n_4, \dots, n_n} |e^{i\theta_{2l}} c_{010n_4 \dots n_n}^{(l)} + e^{i\theta_{1l}} c_{101\bar{n}_4 \dots \bar{n}_n}^{(l)}|^2 \\ & + \sum_{n_4, \dots, n_n} |e^{-i\theta_{2l}} c_{001n_4 \dots n_n}^{(l)} - e^{i\theta_{1l}} c_{110\bar{n}_4 \dots \bar{n}_n}^{(l)}|^2 \\ & \left. + \sum_{n_4, \dots, n_n} |e^{i\theta_{2l}} c_{011n_4 \dots n_n}^{(l)} + e^{i\theta_{1l}} c_{100\bar{n}_4 \dots \bar{n}_n}^{(l)}|^2 \right) \leq \epsilon, \end{aligned}$$

where \bar{n}_i , with $i = 4, 5, \dots, n$, denotes $n_i \oplus 1$. From the above equation, using the steps similar to the ones used to obtain the bound given by Eq. (A23), we obtain a bound on $\sum_l p_l (|c_{0010 \dots 0}^{(l)}|^2 + |c_{1101 \dots 1}^{(l)}|^2)$ as follows:

$$\sum_l p_l (|c_{0010 \dots 0}^{(l)}|^2 + |c_{1101 \dots 1}^{(l)}|^2) \leq \frac{8}{2} \epsilon. \quad (\text{A44})$$

The sum $\sum_{n_1 n_2 \dots n_n \neq 0_1 0_2 \dots 0_n, 1_1 1_2 \dots 1_n} \sum_l p_l |c_{n_1 n_2 \dots n_n}^{(l)}|^2$ can be split into the sum of $(2^{n-1} - 1)$ terms which are a sum of the modulus of two coefficients $c_{n_1 n_2 \dots n_n}^{(l)}$ as in the left-hand side of Eq. (A44). These $(2^{n-1} - 1)$ terms have the same bound as given in Eq. (A44). Therefore, we obtain

$$\sum_l p_l \sum_{n_1 n_2 \dots n_n \neq 0_1 0_2 \dots 0_n, 1_1 1_2 \dots 1_n} |c_{n_1 n_2 \dots n_n}^{(l)}|^2 \leq \frac{8(2^{n-1} - 1)}{2} \epsilon. \quad (\text{A45})$$

Using Eqs. (A42) and (A45) in Eq. (A39), we obtain the bound on the fidelity as given in Theorem 4.

Next, we bound the fidelity of the operators. As in the case of $n = 3$, we also have $\| \{A_1, B_1\} |\psi\rangle \| \leq 4\sqrt{2}\epsilon$ which implies that

$$\begin{aligned} 2^{5-n} \epsilon & \geq \frac{1}{2^n} \| \{A_1, B_1\} |\psi\rangle \|^2 \\ & \geq 1 - \sum_l p_l \cos \theta_l, \end{aligned} \quad (\text{A46})$$

leading to the following bound on the fidelity between \hat{B}_1 and B_1 :

$$F(\hat{B}_1, B_1) \geq 1 - 2^{5-n} \epsilon,$$

employing the similar steps as in the case of $n = 3$. This ends the proof of Theorem 4. ■

APPENDIX B: JORDAN'S LEMMA

In this section we prove a corollary to Jordan's lemma which is a direct generalization of Corollary 7.1 proven in Ref. [32]. For completeness we also state Jordan's lemma (see, e.g., Ref. [32] for a proof).

Lemma 9 (Jordan's lemma). Let A and B be a pair of Hermitian operators acting on a Hilbert space \mathcal{H} such that $A^2 = B^2 = \mathbb{1}$. Then, \mathcal{H} decomposes as a direct sum $\mathcal{H} = \bigoplus_l \mathcal{H}_l$, with $\dim \mathcal{H}_l \in \{1, 2\}$, and A and B act invariantly on each \mathcal{H}_l .

In this way, since the set of eigenvectors of AB span \mathcal{H} , we can decompose the Hilbert space $\mathcal{H} = \bigoplus_l \mathcal{H}_l$ where the dimension of such \mathcal{H}_l is at most 2.

Corollary 1. Let A_i and B_j with $i = 1, 2, 3$ be Hermitian operators acting on a Hilbert space \mathcal{H} that square to identity and satisfy the following commutation relations:

$$[A_i, A_j] = [A_i, B_j] = 0 \quad (i \neq j). \quad (\text{B1})$$

Then, \mathcal{H} can be decomposed as

$$\mathcal{H} = \bigoplus_l (\mathcal{H}_l^1 \otimes \mathcal{H}_l^2 \otimes \mathcal{H}_l^3), \quad (\text{B2})$$

where each local Hilbert space \mathcal{H}_l^i is of dimension at most two. Moreover, $A_1 = \bigoplus_l (A_{1l} \otimes \mathbb{1}_l \otimes \mathbb{1}_l)$, $B_1 = \bigoplus_l (B_{1l} \otimes \mathbb{1}_l \otimes \mathbb{1}_l)$, $A_2 = \bigoplus_l (\mathbb{1}_l \otimes A_{2l} \otimes \mathbb{1}_l)$, $B_2 = \bigoplus_l (\mathbb{1}_l \otimes B_{2l} \otimes \mathbb{1}_l)$, $A_3 = \bigoplus_l (\mathbb{1}_l \otimes \mathbb{1}_l \otimes A_{3l})$, and $B_3 = \bigoplus_l (\mathbb{1}_l \otimes \mathbb{1}_l \otimes B_{3l})$.

Proof. This proof is a direct generalization of that of Corollary 7.1 proven in Ref. [32].

First, let us notice that Eq. (B1) implies that $[A_i B_i, A_j B_j] = 0$ for any $i, j = 1, 2, 3$, which means that all three Hermitian operators $A_i B_i$ can be jointly diagonalized.

Let then $|\alpha, \beta, \gamma\rangle$ be an eigenvector of these operators such that $A_1 B_1 |\alpha, \beta, \gamma\rangle = \alpha |\alpha, \beta, \gamma\rangle$ and $A_2 B_2 |\alpha, \beta, \gamma\rangle = \beta |\alpha, \beta, \gamma\rangle$ and $A_3 B_3 |\alpha, \beta, \gamma\rangle = \gamma |\alpha, \beta, \gamma\rangle$. Define the following vectors: $|\bar{\alpha}, \beta, \gamma\rangle = A_1 |\alpha, \beta, \gamma\rangle$, $|\alpha, \bar{\beta}, \gamma\rangle = A_2 |\alpha, \beta, \gamma\rangle$, $|\alpha, \beta, \bar{\gamma}\rangle = A_3 |\alpha, \beta, \gamma\rangle$, $|\bar{\alpha}, \bar{\beta}, \gamma\rangle = A_1 A_2 |\alpha, \beta, \gamma\rangle$, $|\bar{\alpha}, \beta, \bar{\gamma}\rangle = A_1 A_3 |\alpha, \beta, \gamma\rangle$, $|\alpha, \bar{\beta}, \bar{\gamma}\rangle = A_2 A_3 |\alpha, \beta, \gamma\rangle$, and $|\bar{\alpha}, \bar{\beta}, \bar{\gamma}\rangle = A_1 A_2 A_3 |\alpha, \beta, \gamma\rangle$. Then, the subspace

$$\begin{aligned} & \text{span}\{|\alpha, \beta, \gamma\rangle, |\bar{\alpha}, \beta, \gamma\rangle, |\alpha, \bar{\beta}, \gamma\rangle, |\alpha, \beta, \bar{\gamma}\rangle, \\ & |\bar{\alpha}, \bar{\beta}, \gamma\rangle, |\bar{\alpha}, \beta, \bar{\gamma}\rangle, |\alpha, \bar{\beta}, \bar{\gamma}\rangle, |\bar{\alpha}, \bar{\beta}, \bar{\gamma}\rangle\} \end{aligned} \quad (\text{B3})$$

is isomorphic to $\text{span}\{|\alpha\rangle, |\bar{\alpha}\rangle\} \otimes \text{span}\{|\beta\rangle, |\bar{\beta}\rangle\} \otimes \text{span}\{|\gamma\rangle, |\bar{\gamma}\rangle\}$. It follows from Lemma 9 that both A_1 and B_1 , both A_2 and B_2 , as well as both A_3 and B_3 act invariantly on the first, second, and third tensor factors, and trivially on the others, respectively. ■

The above corollary can be trivially generalized to any $n \geq 3$: let A_i and B_j ($i, j = 1, \dots, n$) be Hermitian operators acting on \mathcal{H}_n that square to the identity and satisfy

$$[A_i, A_j] = [B_i, B_j] = 0 \quad (i \neq j). \quad (\text{B4})$$

Then, \mathcal{H}_n decomposes as $\mathcal{H}_n = \bigoplus_l (\mathcal{H}_l^1 \otimes \mathcal{H}_l^2 \otimes \dots \otimes \mathcal{H}_l^n)$, with $\dim \mathcal{H}_l^i \leq 2$, and

$$A_j = \bigoplus_l \left(\bigotimes_{i=1}^{j-1} \mathbb{1}_l \otimes A_j^l \otimes \bigotimes_{i=j+1}^n \mathbb{1}_l \right) \quad (\text{B5})$$

and

$$B_j = \bigoplus_l \left(\bigotimes_{i=1}^{j-1} \mathbb{1}_l \otimes B_j^l \otimes \bigotimes_{i=j+1}^n \mathbb{1}_l \right). \quad (\text{B6})$$

-
- [1] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [2] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Rev. Mod. Phys.* **79**, 135 (2007).
- [3] P. W. Shor, *Phys. Rev. A* **52**, R2493(R) (1995).
- [4] B. M. Terhal, *Rev. Mod. Phys.* **87**, 307 (2015).
- [5] J. Borregaard, H. Pichler, T. Schröder, M. D. Lukin, P. Lodahl, and A. S. Sørensen, *Phys. Rev. X* **10**, 021071 (2020).
- [6] P. Hilaire, E. Barnes, and S. E. Economou, *Quantum* **5**, 397 (2021).
- [7] B. Lanyon, J. Whitfield, G. Gillett, M. E. Goggin, M. P. Almeida, I. Kassal, J. D. Biamonte, M. Mohseni, B. J. Powell, M. Barbieri, A. Aspuru-Guzik, and A. G. White, *Nat. Chem.* **2**, 106 (2010).
- [8] X. Ma, B. Dakić, W. Naylor, A. Zeilinger, and P. Walther, *Nat. Phys.* **7**, 399 (2011).
- [9] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, *Phys. Rev. Lett.* **98**, 020503 (2007).
- [10] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, *New J. Phys.* **19**, 093012 (2017).
- [11] R. T. Thew, K. Nemoto, A. G. White, and W. J. Munro, *Phys. Rev. A* **66**, 012303 (2002).
- [12] N. Kiesel, C. Schmid, U. Weber, G. Tóth, O. Gühne, R. Ursin, and H. Weinfurter, *Phys. Rev. Lett.* **95**, 210502 (2005).
- [13] J. S. Bell, *Phys. Phys. Fiz.* **1**, 195 (1964).
- [14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Rev. Mod. Phys.* **86**, 419 (2014).
- [15] D. Mayers and A. Yao, *Quantum Inf. Comput.* **4**, 273 (2004).
- [16] I. Šupić and J. Bowles, *Quantum* **4**, 337 (2020).
- [17] J. Kaniewski, *Phys. Rev. Lett.* **117**, 070402 (2016).
- [18] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín, *Phys. Rev. Lett.* **124**, 020402 (2020).
- [19] E. Panwar, P. Pandya, and M. Wieśniak, *arXiv:2202.06908*
- [20] S. Kochen and E. P. Specker, *J. Math. Mech.* **17**, 59 (1967).
- [21] A. J. Leggett and A. Garg, *Phys. Rev. Lett.* **54**, 857 (1985).
- [22] C. Budroni and C. Emary, *Phys. Rev. Lett.* **113**, 050401 (2014).
- [23] S. Brierley, A. Kosowski, M. Markiewicz, T. Paterek, and A. Przysiężna, *Phys. Rev. Lett.* **115**, 120404 (2015).
- [24] C. Budroni, A. Cabello, O. Gühne, M. Kleinmann, and J.-Å. Larsson, *arXiv:2102.13036*.
- [25] M. Markiewicz, A. Przysiężna, S. Brierley, and T. Paterek, *Phys. Rev. A* **89**, 062319 (2014).
- [26] J. Bernejo-Vega, N. Delfosse, D. E. Browne, C. Okay, and R. Raussendorf, *Phys. Rev. Lett.* **119**, 120505 (2017).
- [27] M. Howard, J. Wallman, V. Veitch, and J. Emerson, *Nature (London)* **510**, 351 (2014).
- [28] O. Gühne, C. Budroni, A. Cabello, M. Kleinmann, and J.-Å. Larsson, *Phys. Rev. A* **89**, 062107 (2014).
- [29] C. Spee, H. Siebeneich, T. F. Gloger, P. Kaufmann, M. Johanning, M. Kleinmann, C. Wunderlich, and O. Gühne, *New J. Phys.* **22**, 023028 (2020).
- [30] K. Bharti, M. Ray, A. Varvitsiotis, A. Cabello, and L.-C. Kwek, *arXiv:1911.09448*.
- [31] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L.-C. Kwek, *Phys. Rev. Lett.* **122**, 250403 (2019).
- [32] A. A. M. Irfan, K. Mayer, G. Ortiz, and E. Knill, *Phys. Rev. A* **101**, 032106 (2020).
- [33] D. Saha, R. Santos, and R. Augusiak, *Quantum* **4**, 302 (2020).
- [34] A. G. Maity, S. Mal, C. Jebarathinam, and A. S. Majumdar, *Phys. Rev. A* **103**, 062604 (2021).
- [35] D. E. Gottesman, Ph.D. thesis, California Institute of Technology, 1997.
- [36] D. Schlingemann and R. F. Werner, *Phys. Rev. A* **65**, 012308 (2001).
- [37] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, *Phys. Rev. A* **78**, 042303 (2008).
- [38] M. Ardehali, *Phys. Rev. A* **46**, 5375 (1992).
- [39] A. V. Belinskii and D. N. Klyshko, *Phys. Usp.* **36**, 653 (1993).
- [40] N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).
- [41] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, *Phys. Rev. Lett.* **95**, 120405 (2005).
- [42] G. Tóth, O. Gühne, and H. J. Briegel, *Phys. Rev. A* **73**, 022303 (2006).
- [43] M. Waegell and P. K. Aravind, *Phys. Rev. A* **88**, 012102 (2013).
- [44] D. Gottesman, *Phys. Rev. A* **54**, 1862 (1996).
- [45] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. van den Nest, and H.-J. Briegel, in *Quantum Computers, Algorithms and Chaos, Proceedings of the International School of Physics “Enrico Fermi”, Varenna, 2005*, edited by G. Casati, D. L. Shepelyansky, P. Zoller, and G. Benenti (IOS Press, Amsterdam, 2006), Vol. 162.
- [46] G. Cañas, S. Etcheverry, E. S. Gómez, C. Saavedra, G. B. Xavier, G. Lima, and A. Cabello, *Phys. Rev. A* **90**, 012119 (2014).
- [47] A. Bretto, *Hypergraph Theory*, Mathematical Engineering (Springer, Cham, 2013).
- [48] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, *Quantum* **3**, 198 (2019).
- [49] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, *npj Quantum Inf.* **7**, 151 (2021).
- [50] O. Gühne and A. Cabello, *Phys. Rev. A* **77**, 032108 (2008).
- [51] A. Chaturvedi, M. Farkas, and V. J. Wright, *Quantum* **5**, 484 (2021).

Chapter 4

Paper III

4.1 Scalable Bell inequalities for graph states of arbitrary prime local dimension and self-testing

In the third work forming the thesis we turn to the Bell scenario. We provide a general construction of Bell inequalities whose maximal quantum values are achieved by multipartite graph states of arbitrary prime local dimension which form one of the most representative classes of multipartite entangled states, including for instance the GHZ state, that are a resource for many tasks such as quantum computing. In other words, for any such graph state we provide a Bell inequality maximally violated by this state together with certain quantum observables that correspond to a set of d mutually unbiased bases in prime dimension d . In order to derive these inequalities we build on two other recent constructions of Bell inequalities from Refs. [75] and [22]. Whereas the former work introduces Bell inequalities maximally violated by the maximally entangled states of two qudits with prime local dimension, the latter provides a construction of Bell inequalities tailored to the multiqubit graph states.

Let us notice here that it is in general a difficult task to determine the maximal quantum value of a generic Bell inequality, and, at the same time, Bell inequalities for which the maximal quantum violation is known are highly useful within the area of device-independent quantum information. For instance, maximal Bell violations can be used for certification purposes, in particular in self-testing, but also to certify true randomness [90]. The corresponding Bell operators are constructed with the aid of the stabilizer formalism of the graph states in such a way that we can analytically find their sum-of-squares (SOS) decompositions, which then allows to determine the maximal quantum violations of our Bell inequalities. Importantly, the number of expectation values to measure in order to test the violation of our inequalities scales only linearly with the system size.

Finally, we show that these inequalities can be used for self-testing of multi-qudit graph states such as the well-known four-qudit absolutely maximally entangled state AME(4,3) [91]. Indeed, by employing the results of Ref. [75] we show that in the case of $d = 3$, the algebraic relations implied by the abovementioned SOS decompositions fully characterize two unitarily inequivalent sets of measurements achieving the maximal quantum violation, and, for both of them, the state that attains the optimal violation is the corresponding many-qudit graph state. While we are unable to prove it with the methods at hand, we believe that our inequalities can actually be used to self-test

any qudit graph state for $d \geq 5$.

Our result thus generalizes the self-testing statement made for the qubit graph states in Ref. [22] as well as that of Ref. [75] made for the two-qutrit maximally entangled state. In fact, our proof of the self-testing statement heavily exploits the results of the latter work. The possibilities of future work are discussed in the Conclusions section of the article.

4.2 Author's contribution

My contribution to this article was:

- Active participation in discussions that lead to designing the main idea of the work and to finding a way to derive the Bell inequalities;
- Signification contribution in deriving the Bell inequalities for graph states and proving Theorem 2;
- Help in proving the self-testing statement in Theorem 3;
- Help in preparing the manuscript.

PAPER • OPEN ACCESS

Scalable Bell inequalities for graph states of arbitrary prime local dimension and self-testing

To cite this article: Rafael Santos *et al* 2023 *New J. Phys.* **25** 063018

View the [article online](#) for updates and enhancements.



OPEN ACCESS

RECEIVED

19 December 2022

REVISED

4 May 2023

ACCEPTED FOR PUBLICATION

30 May 2023

PUBLISHED

20 June 2023

Original Content from
this work may be used
under the terms of the
[Creative Commons
Attribution 4.0 licence](#).

Any further distribution
of this work must
maintain attribution to
the author(s) and the title
of the work, journal
citation and DOI.



PAPER

Scalable Bell inequalities for graph states of arbitrary prime local dimension and self-testing

Rafael Santos¹, Debashis Saha², Flavio Baccari³ and Remigiusz Augusiak^{1,*} ¹ Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland² School of Physics, Indian Institute of Science Education and Research Thiruvananthapuram, Thiruvananthapuram, Kerala 695551, India³ Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, 85748 Garching, Germany

* Author to whom any correspondence should be addressed.

E-mail: augusiak@cft.edu.pl**Keywords:** Bell non-locality, Bell inequalities, quantum entanglement, multipartite states, graph states, self-testing

Abstract

Bell nonlocality—the existence of quantum correlations that cannot be explained by classical means—is certainly one of the most striking features of quantum mechanics. Its range of applications in device-independent protocols is constantly growing. Many relevant quantum features can be inferred from violations of Bell inequalities, including entanglement detection and quantification, and state certification applicable to systems of arbitrary number of particles. A complete characterisation of nonlocal correlations for many-body systems is, however, a computationally intractable problem. Even if one restricts the analysis to specific classes of states, no general method to tailor Bell inequalities to be violated by a given state is known. In this work we provide a general construction of Bell expressions tailored to the graph states of any prime local dimension. These form a broad class of multipartite quantum states that have many applications in quantum information, including quantum error correction. We analytically determine their maximal quantum values, a number of high relevance for device-independent applications of Bell inequalities. Importantly, the number of expectation values to determine in order to test the violation of our inequalities scales only linearly with the system size, which we expect to be the optimal scaling one can hope for in this case. Finally, we show that these inequalities can be used for self-testing of multi-qutrit graph states such as the well-known four-qutrit absolutely maximally entangled state AME(4,3).

1. Introduction

The first Bell inequalities were introduced to show that certain predictions of quantum theory cannot be explained by classical means [1]. In particular, correlations obtained by performing local measurements on joint entangled quantum states are able to violate Bell inequalities and hence cannot arise from a local hidden variable model. The existence of such non-local correlations is referred to as Bell non-locality or simply non-locality.

Since then the range of applications of Bell inequalities has become much wider. In particular, they can be used for certification of certain relevant quantum properties in a device-independent way, that is, under minimal assumptions about the underlying quantum system. First, violation of Bell inequalities can be used to certify the dimension of a quantum system [2] or the amount of entanglement present in it [3]. Then, Bell violations are used to certify that the outcomes of quantum measurements are truly random [4], and to estimate the amount of generated randomness [5–7].

The maximum exponent of the certification power of Bell inequalities is known as self-testing. Introduced in [8], self-testing allows for almost complete characterisation of the underlying quantum system

based only on the observed Bell violation. It thus appears to be one of the most accurate methods for certification of quantum systems which makes self-testing a highly valuable asset for the rapidly developing of quantum technologies. In fact, self-testing techniques have shown to be amenable for near-term quantum devices, allowing for a proof-of-principle state certification of up to few tens of particles [9, 10]. For this reason self-testing has attracted a considerable attention in recent years (see, e.g. [11]).

However, most of the above applications require Bell inequalities that exhibit carefully crafted features. In the particular case of self-testing one needs Bell inequalities whose maximal quantum values are achieved by the target quantum state and measurements that one aims to certify. Deriving Bell inequalities tailored to generic pure entangled states turns out to be in general a difficult challenge. Even more so if one looks for inequalities applicable to systems of arbitrary number of parties or arbitrary local dimension. The standard geometric approach to derive Bell inequalities has been successful in deriving many interesting and relevant inequalities [12–16], but typically fails to serve a self-testing purpose, providing inequalities with unknown maximal quantum violation.

In order to construct Bell inequalities that are tailored to specific quantum states, a more promising path is to exploit the ‘quantum properties’ of the considered system such as its symmetries. Two proposals in this direction have succeeded in designing different classes of Bell inequalities tailored to the broad family of multi-qubit graph states [17, 18] and the first Bell inequalities maximally violated by the maximally entangled state of any local dimension [19]. The success of these methods was further confirmed by later applications to design the first self-testing Bell inequalities for graph states [20] (see also [21] for the first self-testing method for multi-qubit graph states which, however, is not directly based on violation of Bell inequalities), for genuinely entangled stabilizer subspaces [22, 23] or maximally entangled two-qutrit states [24], as well as to derive many other classes of Bell inequalities tailored to two-qudit maximally entangled [25, 26] or many-qudit Greenberger–Horne–Zeilinger (GHZ) states [27]. Some of these constructions were later exploited to provide self-testing schemes for the maximally entangled [25, 28] or the GHZ states [29] of arbitrary local dimension.

In this work, taking inspiration from the above ideas, we provide the first general construction of Bell expressions tailored to graph states of arbitrary prime local dimension. Graph states constitute one of the most representative classes of genuinely entangled multipartite quantum states considered in quantum information, covering the well-known GHZ, the cluster [30] or the absolutely maximally entangled states [31], that have found numerous applications, e.g. in quantum computing [32–34] or quantum metrology [35]. We analytically determine the maximal quantum value (called also Tsirelson’s bound) of each of our Bell expressions by deriving a suitable sum-of-squares decomposition of the corresponding Bell operator. We then show that this maximal value is achieved by the corresponding graph state. On the other hand, the maximal classical values of our Bell expressions are yet to be determined. We nevertheless believe that our inequalities are all nontrivial in the sense that their maximal quantum and classical values differ. In fact, in the particular case of $d = 3$ we prove that they all allow for self-testing of the corresponding graph states, and thus are certainly nontrivial in the above sense. Moreover, for the simplest bipartite graph corresponding to the maximally entangled state of two qudits, the maximal classical value can be determined numerically for the lowest values of d and it differs from the corresponding Tsirelson’s bound (see [24]). We thus believe that all our Bell expressions feature this property and therefore in what follows, slightly abusing the terminology, we also refer to them as to Bell inequalities.

Our construction thus provides the first example of Bell inequalities maximally violated by the absolutely maximally entangled states of non-qubit local dimension such as the four-qutrit AME(4,3) state [31]. Our Bell expressions are also scalable because the number of expectation values they are composed of scales only linearly with the number of subsystems, which we expect to be the optimal scaling in the case of graph states. This is a relevant factor as far as experimental tests of Bell non-locality or implementations of self-testing are concerned; by lowering the number of expectation values one can lower the experimental effort to test a Bell inequality violation. Let us finally notice that our construction generalizes and unifies in a way the recent constructions of [20] and [24] to all graph states of arbitrary prime local dimension.

The manuscript is organized as follows. In section 2 we provide some background information which is necessary for further considerations; in particular we explain in detail the notions of the multipartite Bell scenario and graph states and also state the definition of self-testing we use in our work. Next, in section 3 we introduce our general construction of Bell expressions for graph states. We then show in section 4 that our new Bell inequalities allow for self-testing of all graph states of local dimension three. We conclude in section 5 where we also provide a list of possible research directions for further studies that follow from our work.

2. Preliminaries

2.1. Bell scenario and Bell inequalities

Let us begin by introducing some notions and terminology. We consider a multipartite Bell scenario in which N distant observers A_i share a quantum state ρ defined on the product Hilbert space

$$\mathcal{H} = \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_N. \quad (1)$$

Each observer A_i can perform one of m_i measurements $M_{x_i}^i \equiv \{M_{a_i|x_i}^i\}_{a_i}$ on their share of this state, where x_i stand for the measurement choices, whereas a_i denote the outcomes; here we label them as $x_i = 1, \dots, m$ and $a_i = 0, \dots, d-1$, respectively. Recall that the measurement operators satisfy $M_{a_i|x_i}^i \geq 0$ for any choice of a_i and x_i as well as $\sum_{a_i} M_{a_i|x_i}^i = \mathbb{1}$ for any x_i .

The observers repeat their measurements on the local parts of the state ρ which creates correlations between the obtained outcomes. These are captured by a collection of probability distributions $\vec{p} \equiv \{p(\vec{a}|\vec{x})\} \in \mathbb{R}^{(md)^N}$, where $p(\vec{a}|\vec{x}) \equiv p(a_1, \dots, a_N | x_1, \dots, x_N)$ is the probability of obtaining the outcome a_i by the observer i upon performing the measurement $M_{x_i}^i$ and can be represented by the Born rule

$$p(\vec{a}|\vec{x}) = \text{Tr} \left[\rho \left(M_{a_1|x_1}^1 \otimes \dots \otimes M_{a_N|x_N}^N \right) \right]. \quad (2)$$

A behaviour \vec{p} is said to be local or classical if for any \vec{a} and \vec{x} , the joint probabilities $p(\vec{a}|\vec{x})$ factorize in the following sense,

$$p(\vec{a}|\vec{x}) = \sum_{\lambda} \mu(\lambda) p_1(a_1|x_1, \lambda) \dots p_N(a_N|x_N, \lambda), \quad (3)$$

where λ is a random variable with a probability distribution $\mu(\lambda)$ representing the possibilities for the parties to share classical correlations and $p_i(a_i|x_i, \lambda)$ is an arbitrary probability distribution corresponding to the observer A_i . On the other hand, if a behavior \vec{p} does not admit the above form, we call it Bell non-local or simply non-local. In any Bell scenario correlations that are classical in the above sense form a polytope with finite number of vertices, denoted $L_{N,m,d}$.

Any non-local distribution \vec{p} can be detected to be outside the local polytope from the violation of a Bell inequality. The generic form of such inequalities is

$$I := \sum_{\vec{a}, \vec{x}} \alpha_{\vec{a}, \vec{x}} p(\vec{a}|\vec{x}) \leq \beta_L, \quad (4)$$

where $\beta_L = \max_{\vec{p} \in L_{N,m,d}} I$ is the classical bound of the inequality and $\alpha_{\vec{a}, \vec{x}}$ are some real coefficients defining the inequality. Any \vec{p} that violates a Bell inequality is detected as non-local.

Let us finally introduce another number characterizing a Bell inequality—the so-called quantum or Tsirelson's bound—which is defined as

$$\beta_Q = \sup_{\vec{p} \in Q_{N,m,d}} I, \quad (5)$$

where the maximisation runs on all quantum behaviours, i.e. all distributions \vec{p} that can be obtained by performing quantum measurements on quantum states of arbitrary local dimension. The set of quantum correlations $Q_{N,m,d}$ is in general not closed [36] and thus β_Q is a supremum and not a strict maximum. Determining the quantum bound for a generic Bell inequality is an extremely difficult problem. However, interestingly, in certain cases it can still be found analytically. A way to obtain β_Q or at least an upper bound on it is to find a sum-of-squares decomposition of a Bell operator \mathcal{B} corresponding to the Bell inequality. More specifically, if for any choice of measurement operators one is able to represent the Bell operator as

$$\mathcal{B} = \eta \mathbb{1} - \sum_k P_k^\dagger P_k, \quad (6)$$

where P_k are some operators composed of $M_{n_i|x_i}^i$, then η is an upper bound on β_Q . Indeed, equation (6) implies that for all $|\psi\rangle$, $\langle \psi | \mathcal{B} | \psi \rangle \leq \eta$, and thus, $\beta_Q \leq \eta$. If a quantum state saturates this upper bound, then it follows from (6) that $P_k |\psi\rangle = 0$ for all k . As we will see later such relations are particularly useful to prove a self-testing statement from the maximal violation of a Bell inequality.

For further convenience we also introduce an alternative description of the Bell scenario in terms of generalized expectation values (see, e.g. [27]). These are in general complex numbers defined through the N -dimensional discrete Fourier transform of $\{p(\vec{a}|\vec{x})\}$,

$$\langle A_{n_1|x_1}^1 \dots A_{n_N|x_N}^N \rangle = \sum_{\vec{a}} \omega^{\vec{a} \cdot \vec{n}} p(\vec{a}|\vec{x}), \quad (7)$$

where $\omega = \exp(2\pi i/d)$ is the d th root of unity, $\vec{a} := (a_1, \dots, a_N) \in \{0, \dots, d-1\}^N$ and $\vec{n} := (n_1, \dots, n_N) \in \{0, \dots, d-1\}^N$, and $\vec{a} \cdot \vec{n} = \sum_i a_i n_i$. The inverse transformation gives

$$p(\vec{a}|\vec{x}) = \frac{1}{d^N} \sum_{\vec{n}} \omega^{-\vec{a} \cdot \vec{n}} \langle A_{n_1|x_1}^1 \dots A_{n_N|x_N}^N \rangle. \quad (8)$$

Combining equations (2) and (8) one finds that if the correlations \vec{p} are quantum, that is, originate from performing local measurements on composite quantum states, the complex expectation values can be represented as

$$\langle A_{n_1|x_1}^1 \dots A_{n_N|x_N}^N \rangle = \text{Tr} \left[\rho \left(A_{n_1|x_1}^1 \otimes \dots \otimes A_{n_N|x_N}^N \right) \right], \quad (9)$$

where $A_{n_i|x_i}^i$ are simply Fourier transforms of the measurement operators $M_{a_i|x_i}^i$ given by

$$A_{n_i|x_i}^i = \sum_{a_i=0}^{d-1} \omega^{n_i a_i} M_{a_i|x_i}^i. \quad (10)$$

Clearly, due to the fact that the Fourier transform is invertible, for a given x_i and i , the d operators $A_{n_i|x_i}^i$ with $n_i = 0, \dots, d-1$ uniquely represent the corresponding measurement $M_{x_i}^i$.

Let us now discuss a few properties of the Fourier-transformed measurement operators that will prove very useful later. For clarity of the presentation we consider a single quantum measurement $M = \{M_a\}$ and the corresponding A_n operators obtained via equation (10). First, one easily finds that $A_0 = \mathbb{1}$. Second,

$$A_{d-n} = A_{-n} = A_n^\dagger \quad (11)$$

which is a consequence of the fact that $\omega^{d-n} = \omega^{-n} = (\omega^n)^*$ holds true for any $n \in \{0, \dots, d-1\}$. Third, $A_n^\dagger A_n \leq \mathbb{1}$ for any $n = 0, \dots, d-1$ (for a proof see [24]).

Let us finally mention that if M is projective then all A_n are unitary and their eigenvalues are simply the powers of ω ; equivalently $A_n^d = \mathbb{1}$. It is also not difficult to see that in such a case, A_n are operator powers of A_1 , that is, $A_n = A_1^n$. Thus, a projective measurement can be represented by a single unitary (non-Hermitian for $d \geq 3$) operator A_1 , which by slightly abusing the standard terminology we call here quantum observable. We exploit these properties later in our construction of Bell expressions as well as in deriving the self-testing statement. In fact, in what follows we denote the observables measured by the party i by A_{i,x_i} .

2.2. Self-testing

Here we introduce the definition of N -partite self-testing that we adopt in this work. Let us consider again the Bell scenario described above, assuming, however, that the shared state ρ , the Hilbert space it acts on as well as the local measurements are all unknown. The aim of the parties is to deduce their form from the observed correlations $p(\vec{a}|\vec{x})$. Since the dimension of the joint Hilbert space \mathcal{H} is now unconstrained (although finite) we can simplify the latter problem by assuming that the shared state is pure, i.e. $\rho = |\psi\rangle\langle\psi|$ for some $|\psi\rangle \in \mathcal{H}$, and the measurements are projective, in which case they are represented by unitary observables A_{i,x_i} acting on \mathcal{H}_i .

Consider then a target state $|\hat{\psi}\rangle \in (\mathbb{C}^d)^{\otimes N}$ and the corresponding measurements \hat{A}_{i,x_i} , giving rise to the same behaviour $\{p(\vec{a}|\vec{x})\}$. We say that the observed correlations self-test the given state and measurements if the following definition applies.

Definition 1. If from the observed correlations $\{p(\vec{a}|\vec{x})\}$ one can identify a qudit in each local Hilbert space in the sense that $\mathcal{H}_i = \mathbb{C}^d \otimes \mathcal{H}'_i$ for some auxiliary Hilbert space \mathcal{H}'_i , and also deduce the existence of local unitary operations $U_i : \mathcal{H}_i \rightarrow \mathbb{C}^d \otimes \mathcal{H}'_i$ such that

$$(U_1 \otimes \dots \otimes U_N)|\psi\rangle = |\hat{\psi}\rangle \otimes |\text{aux}\rangle \quad (12)$$

for some $|\text{aux}\rangle \in \mathcal{H}'_i \otimes \dots \otimes \mathcal{H}'_N$, and, moreover,

$$U_i A_{i,x_i} U_i^\dagger = \hat{A}_{i,x_i} \otimes \mathbb{1}_i, \quad (13)$$

where $\mathbb{1}_i$ is the identity acting on \mathcal{H}'_i , then we say that the reference quantum state $|\hat{\psi}\rangle$ and measurements \hat{A}_{i,x_i} have been self-tested in the experiment.

Importantly, only non-local correlations can give rise to a valid self-testing statement. Moreover, since it is based only on the observed correlations $\{p(\vec{a}|\vec{x})\}$, self-testing can characterise the state and the measurements only up to certain equivalences. In particular, the statement above includes two possible operations that keep the correlations $\{p(\vec{a}|\vec{x})\}$ unchanged: (i) the addition of an auxiliary state $|\text{aux}\rangle$ on which the measurements act trivially and (ii) the rotation by an arbitrary local unitary operations. It is worth mentioning, however, that there exist yet another operation that does not change $\{p(\vec{a}|\vec{x})\}$, which is the transposition map applied to the state and all the measurements. Taking into account this extra degree of freedom would lead to a weaker definition of self-testing than the one formulated above (see, e.g. [24, 37]). Since in our work we are concerned only with self-testing of the graph states, which are real and thus invariant under the action of transposition, we do not need to take into account this other definition of self-testing.

2.3. Graph states

Let us finally recall the definition of multipartite graph states of prime local dimension [38–40]. Consider a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{R}, d)$, where d is any prime number such that $d \geq 2$, $\mathcal{V} := \{1, \dots, N\}$ is the set of vertices of the graph, \mathcal{E} is the set of edges connecting vertices, and $\mathcal{R} := \{r_{i,j}\}$ is a set of natural numbers from $\{0, \dots, d-1\}$ specifying the number of edges connecting vertices $i, j \in \mathcal{V}$; in particular, $r_{i,j} = 0$ means there is no edge between i and j . We additionally assume that $r_{i,i} = 0$ for all i , meaning that the graph has no loops as well as that the graph \mathcal{G} is connected, meaning that it does not have any isolated vertices. By \mathcal{N}_i we denote the neighbourhood of the vertex i which consists of all elements of \mathcal{V} that are connected to i .

Assume then that each vertex $i \in \mathcal{V}$ of the graph corresponds to a single quantum system held by the party A_i and let us associate to it the following N -qudit operator

$$G_i = X_i \otimes \bigotimes_{j \in \mathcal{N}_i} Z_j^{r_{ij}} \quad (i = 1, \dots, N) \quad (14)$$

with X and Z being the generalizations of the qubit Pauli matrices to d -dimensional Hilbert spaces defined via the following relations

$$Z|i\rangle = \omega^i|i\rangle, \quad X|i\rangle = |i+1\rangle \quad (i = 0, \dots, d-1), \quad (15)$$

where the addition is modulo d . Due to the fact that $XZ = \omega^{-1}ZX$, it is not difficult to see that the operators G_i mutually commute. It then follows that there is a unique pure state $|G\rangle \in (\mathbb{C}^d)^{\otimes N}$, called graph state, which is a common eigenstate of all G_i corresponding to the eigenvalue one, i.e.

$$G_i|G\rangle = |G\rangle \quad (i = 1, \dots, N). \quad (16)$$

Given the above property, the G_i are usually referred to as stabilizing operators. Notice also that in the particular case of $d = 2$ this construction naturally reproduces the N -qubit graph states [40], where vertices can only be connected by single edges.

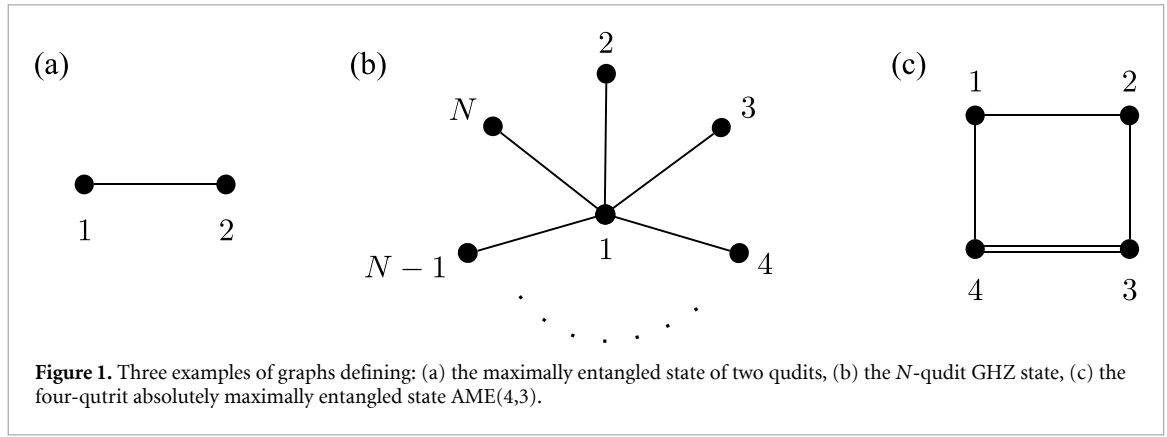
Let us illustrate the above construction with a couple of examples.

Example 1 (Maximally entangled two-qudit state). Let us start with the simplest possible graph, consisting of two vertices connected by an edge (cf figure 1(a)). The corresponding generators are given by

$$G_1 = X \otimes Z, \quad G_2 = Z \otimes X, \quad (17)$$

and stabilize a single state in $\mathbb{C}^d \otimes \mathbb{C}^d$ which is equivalent up to local unitary operations to the maximally entangled state of two qudits,

$$|\psi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle \quad (18)$$



in which both local Schmidt bases are the computational one. In fact, the above state is stabilized by another pair of operators, namely,

$$G'_1 = X \otimes X, \quad G'_2 = Z \otimes Z^\dagger, \quad (19)$$

which are obtained from G_i by an application of the Fourier matrix to the second site.

Example 2 (GHZ state). The above two-vertex graph naturally generalizes to a star graph consisting of N vertices (cf figure 1(b)). The associated generators are of the form

$$G_1 = X_1 Z_2 \dots Z_N \quad (20)$$

and

$$G_i = Z_1 X_i \quad (i = 2, \dots, N), \quad (21)$$

and stabilize an N -qudit state which is equivalent under local unitary operations to the well-known GHZ state

$$|\text{GHZ}_{N,d}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes N}. \quad (22)$$

Example 3 (AME(4,3)). The third and the last example is concerned with the four-qudit absolutely maximally entangled state⁴, named AME(4,3) [31]. The graph defining it is presented in figure 1(c). The stabilizing operators corresponding to this graph read

$$G_1 = X_1 Z_2 Z_4, \quad G_2 = Z_1 X_2 Z_3, \quad G_3 = Z_2 X_3 Z_4^2, \quad G_4 = Z_1 Z_3^2 X_4. \quad (23)$$

They stabilize a three-qudit maximally entangled state AME(4,3) which is equivalent under local unitary operations and relabelling of the subsystems to (see, e.g. [42]),

$$|\text{AME}(4,3)\rangle = \frac{1}{3} \sum_{i,j=0}^2 |i\rangle |j\rangle |i+j\rangle |i+2j\rangle, \quad (24)$$

where the addition is modulo three.

3. Construction of Bell inequalities for arbitrary graph states of prime local dimension

Here we present our first main result: a general construction of Bell expressions whose maximal quantum value is achieved by the N -qudit graph states of arbitrary prime local dimension and quantum observables corresponding to mutually unbiased bases at every site. Our construction is inspired by the recent approach to construct CHSH-like Bell inequalities for the N -qubit graph states presented in [20] and by another

⁴ A multipartite state is termed absolutely maximally entangled if any of its $\lfloor N/2 \rfloor$ -partite subsystems is in the maximally mixed state [41].

construction of Bell inequalities maximally violated by the maximally entangled two-qudit state introduced in [24].

First, in section 3.1 we recall the general class of Bell inequalities maximally violated by N -qubit graph states of [20]. Then, in section 3.2 we introduce the main building block to generalise this construction to arbitrary prime dimension. We illustrate the Bell inequality construction with some simple examples in section 3.3 and then move to introduce the general form of the inequality valid of any N -qudit graph state of prime dimension in section 3.4.

3.1. Multiqubit graph states

Let us assume that $d = 2$ and let us consider a graph \mathcal{G} . Without any loss of generality we can assume that a vertex with the largest neighbourhood is the first one, that is, $N_1 = \max_{i=1,\dots,N} |\mathcal{N}_i|$. If there are many vertices with the maximal neighbourhood in \mathcal{G} , we are free to choose any of them as the first one.

To every generator G_i we associate an expectation value in which the X and Z Pauli matrices are replaced by quantum observables or their combinations using the following rule. At the first qubit we make the following assignment,

$$X \rightarrow \frac{1}{\sqrt{2}}(A_{1,0} + A_{1,1}), \quad Z \rightarrow \frac{1}{\sqrt{2}}(A_{0,1} - A_{1,1}), \quad (25)$$

whereas the Pauli matrices at the remaining sites are directly replaced by observables, that is,

$$X \rightarrow A_{i,0}, \quad Z \rightarrow A_{i,1} \quad (26)$$

with $i = 2, \dots, N$. Recall that the first index enumerates the parties, while the second one measurement choices. This procedure gives us N expectation values which after being combined altogether lead us to the following Bell inequality [20]:

$$\begin{aligned} I_G := & \frac{N_1}{\sqrt{2}} \left\langle (A_{1,0} + A_{1,1}) \prod_{i \in \mathcal{N}(1)} A_{i,1} \right\rangle + \frac{1}{\sqrt{2}} \sum_{i \in \mathcal{N}(1)} \left\langle (A_{1,0} - A_{1,1}) A_{i,0} \prod_{j \in \mathcal{N}(1) \setminus \{1\}} A_{j,1} \right\rangle \\ & + \sum_{i \notin \mathcal{N}(1) \cup \{1\}} \left\langle A_{i,0} \prod_{j \in \mathcal{N}(i)} A_{j,1} \right\rangle \leq \beta_C^G, \end{aligned} \quad (27)$$

where the classical bound can directly be determined for any graph G and is given by $\beta_C^G = N + (\sqrt{2} - 1)N_1 - 1$. More importantly, the maximal quantum value can also be analytically computed for any graph and amounts to $\beta_Q^G = N + N_1 - 1$. This value is achieved by the graph state $|G\rangle \in (\mathbb{C}^2)^{\otimes N}$ corresponding to the graph \mathcal{G} and the following observables:

$$A_{1,0} = \frac{1}{\sqrt{2}}(X + Z), \quad A_{1,1} = \frac{1}{\sqrt{2}}(X - Z) \quad (28)$$

for the first observer and $A_{i,0} = X$ and $A_{i,1} = Z$ for the remaining observers $i = 2, \dots, N$.

It is worth stressing here that one of the key observations making the construction of [20] work is that for any graph there exists a choice of observables at any site, given by the above formulas, turning the quantum operators appearing in the expectation values of (27) into the stabilising operators G_i ; in particular, it is a well-known fact that combinations of the Pauli matrices in equation (28) are proper quantum observables with eigenvalues ± 1 . Let us also mention that the replacement in equations (25) and (26) guarantees that the maximal quantum and classical values of the inequalities (27) can be determined basically by hand and that they differ for any graph state, implying that all these inequalities are nontrivial.

3.2. Replacement rule for operators of arbitrary prime dimension

We now move on to introduce the main ingredient needed to generalise the above construction to graph states of prime local dimension $d \geq 3$.

A naive approach to constructing Bell inequalities for graph states of higher local dimensions would be to directly follow the $d = 2$ strategy. That is, at a chosen site the X and Z operators are replaced by combinations of general d -outcome observables A_0 and A_1 . However, this simple approach fails to work beyond $d = 3$ because for any prime $d \geq 3$ it is impossible find nonzero complex numbers $\alpha, \beta \in \mathbb{C}$ for which

$$O = \alpha X + \beta Z, \quad (29)$$

is a valid quantum observable; in fact, for no complex numbers the above combinations can be unitary, unless $d = 2$ (cf fact 2 in appendix A). This makes the transformation (28) irreversible. Phrasing differently,

there are no unitary observables A_0 and A_1 such that $X = \alpha A_0 + \beta A_1$ and $Z = \delta A_0 + \gamma A_1$ for some complex numbers $\alpha, \beta, \gamma, \delta \in \mathbb{C}$.

Nevertheless, there exist other sets of d -outcome quantum observables which can be linearly combined to form quantum observables, and thus are convenient for our purposes. One such choice is the following set of d unitary matrices

$$O_k := XZ^k \quad (k = 0, \dots, d-1). \quad (30)$$

It is not difficult to check that $O_k^d = \mathbb{1}_d$ for any $k = 0, \dots, d-1$ and prime d , meaning that the eigenvalues of each of these unitary matrices belong to the set $\{1, \omega, \dots, \omega^{d-1}\}$, and thus are proper d -outcome observables in our formalism. It is also worth mentioning that for any prime $d \geq 2$ their eigenvectors together with the standard basis in \mathbb{C}^d form $d+1$ mutually unbiased bases.

Let us now assume that d is a prime number greater than two ($d \geq 3$) and consider the following linear combinations of O_k and their powers,

$$\overline{O}_x^{(n)} = \frac{\lambda_n}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{nxk} \omega^{nk(k+1)} O_k^n, \quad (31)$$

where $x = 0, 1, \dots, d-1$ and λ_n are complex coefficients defined as [24]:

$$\lambda_n = \left[\varepsilon_d \left(\frac{n}{d} \right) \right]^{-1} \omega^{-g(n,d)/48}, \quad (32)$$

where

$$\varepsilon_d := \begin{cases} 1, & \text{if } d \equiv 1 \pmod{4}, \\ i, & \text{if } d \equiv 3 \pmod{4}. \end{cases} \quad (33)$$

$\left(\frac{n}{d} \right)$ is the Legendre symbol⁵, and, finally, the coefficients $g(n, d)$ are given by

$$g(n, d) = \begin{cases} n[n^2 - d(d+6) + 3] & \text{if } n \equiv 0 \pmod{2} \text{ and } n + d + 1/2 \equiv 0 \pmod{2}, \\ n[n^2 - d(d-6) + 3] & \text{if } n \equiv 0 \pmod{2} \text{ and } n + d + 1/2 \equiv 1 \pmod{2}, \\ n(n^2 + 3) + 2d^2(-5n + 3) & \text{if } n \equiv 1 \pmod{4}, \\ n(n^2 + 3) + 2d^2(n + 3) & \text{if } n \equiv 3 \pmod{4}. \end{cases} \quad (34)$$

Importantly, it was proven in [24] (see appendix D therein) that $\overline{O}_x^{(n)}$ are unitary and satisfy

$$\left[\overline{O}_x^{(n)} \right]^d = \mathbb{1}_d \quad (35)$$

for any $x = 0, \dots, d-1$ and $n = 1, \dots, d-1$. What is more, $\overline{O}_x^{(n)}$ turns out to be the n th power of \overline{O}_x , that is, $\overline{O}_x^{(n)} = [\overline{O}_x]^n$. All this means that for any x the set $\{\overline{O}_x^{(n)}\}_{n=0, \dots, d-1}$ represents a legitimate d -outcome projective quantum measurement. Let us finally mention that the linear transformation (31) can be inverted, giving

$$O_l^n = \frac{\omega^{-nl(l+1)}}{\sqrt{d}\lambda_n} \sum_{x=0}^{d-1} \omega^{-nxl} \overline{O}_x^{(n)}. \quad (36)$$

The fact that both O_k and \overline{O}_k are unitary quantum observables that are related by a linear reversible transformation given by equations (31) and (36) is the key ingredient in our construction. That is, we can proceed in analogy to $d=2$ case, where we used the replacement defined in equation (25) to define the Bell inequality and we could later reverse it by a suitable choice of quantum observables (28) to obtain the maximal quantum violation with a graph state.

The replacement rule we use for the case of arbitrary prime dimension becomes:

$$(XZ^k)^n \rightarrow \tilde{A}_k^{(n)} := \frac{\omega^{-nk(k+1)}}{\sqrt{d}\lambda_n} \sum_{t=0}^{d-1} \omega^{-ntk} A_t^n, \quad (37)$$

⁵ Recall that the Legendre symbol $\left(\frac{n}{d} \right)$ equals +1 if n is a quadratic residue modulo d and -1 otherwise.

where A_t with $t = 0, \dots, d-1$ are unitary observables. Notice that since we deal now with d -outcome quantum measurements we need to also take into account the powers n of the corresponding observables. In fact, these under the Fourier transform represent the outcomes of projective measurements. Crucially, this transformation can be inverted in the sense that there exist a choice of observables $A_{i,t}$,

$$A_t^n = \frac{\lambda_n}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{nk} \omega^{nk(k+1)} (XZ^k)^n. \quad (38)$$

for which $\tilde{A}_k^{(n)}$ in equation (37) can be brought back to XZ^k .

These new operators $\tilde{A}_k^{(n)}$ satisfy the following relations (see fact 3 in appendix A for a proof):

$$\left(\tilde{A}_k^{(n)}\right)^\dagger = \tilde{A}_k^{(d-n)} = \tilde{A}_k^{(-n)} \quad (39)$$

for any pair $n, k = 0, \dots, d-1$, and

$$\sum_{k=0}^{d-1} \tilde{A}_k^{(d-n)} \tilde{A}_k^{(n)} = d\mathbb{1} \quad (40)$$

for any $n = 0, \dots, d-1$.

The motivation for considering the above replacement rule to construct Bell inequalities tailored to multi-qudit graph states stems from a few facts. First, the same rule was already used in [24] to derive Bell inequalities maximally violated by the two-qudit maximally entangled states, which are the simplest examples of the graph states. Second, the same rule in the simplest case of $d = 2$, outlined also in section 3.1, allowed to construct nontrivial Bell inequalities for all multi-qubit graph states. We thus believe that, similarly to the case $d = 2$, the assignment (37) prevents the local models achieve the maximal quantum values of the resulting Bell expression. It also allows, as evidenced in [24], to easily construct sum-of-squares decompositions of our inequalities, and thus analytically determine their maximal quantum values.

3.3. Examples

Before presenting our construction in full generality, let us first illustrate how to use the qudit replacement rule to obtain valid Bell inequalities tailored to graph states by means of two examples.

Example 1 (AME(4,3)). As mentioned in section 2.3, the four-qudit absolutely maximally entangled state is a graph state corresponding to the graph presented on figure 1. The stabilizing operators defining this state are given in equation (23). We recall them here

$$G_1 = X_1 Z_2 Z_4, \quad G_2 = Z_1 X_2 Z_3, \quad G_3 = Z_2 X_3 Z_4^2, \quad G_4 = Z_1 Z_3^2 X_4. \quad (41)$$

Since the neighbourhood of all vertices of this graph is of size two, each vertex is equally good to implement the transformation (37). For simplicity we choose it to be the first site. Moreover, as in the previous example, we denote the observables measured by the four parties as A_x , B_y , etc.

Now, to create the set of matrices XZ^k (necessary for the transformation (37)) at the first site we consider the stabilizing operators G_1 , $G_1 G_2$, and $G_1 G_2^2$. These are, however, insufficient to uniquely define $|\text{AME}(4,3)\rangle$ as they do not include G_3 and G_4 . Since G_3 has the identity at the first position we can include it as it is, whereas we need to take a product of G_4 with G_1 to create XZ at the first site. As a result, the final set of stabilising operators which we use to construct a Bell inequality for $|\text{AME}(4,3)\rangle$ consists of

$$\begin{aligned} G_1 &= X \otimes Z \otimes \mathbb{1} \otimes Z, \\ G_1 G_2 &= XZ \otimes ZX \otimes Z \otimes Z, \\ G_1 G_2^2 &= XZ^2 \otimes ZX^2 \otimes Z^2 \otimes Z, \\ G_3 &= \mathbb{1} \otimes Z \otimes X \otimes Z^2 \\ G_1 G_4 &= XZ \otimes Z \otimes Z^2 \otimes ZX. \end{aligned} \quad (42)$$

Now, to each of these stabilising operators we associate an expectation value in which particular matrices are replaced by quantum observables or their combinations. For pedagogical purposes, let us do it site by site. As already mentioned, at the first site we use equation (37) which for $d = 3$ gives

$$\begin{aligned}
X &\rightarrow \tilde{A}_0 := \frac{1}{\sqrt{3}\lambda_1} (A_0 + A_1 + A_2), \\
XZ &\rightarrow \tilde{A}_1 := \frac{1}{\sqrt{3}\lambda_1\omega} (A_0 + \omega^{-1}A_1 + \omega^{-2}A_2), \\
XZ^2 &\rightarrow \tilde{A}_2 := \frac{1}{\sqrt{3}\lambda_1} (A_0 + \omega^{-2}A_1 + \omega^{-1}A_2),
\end{aligned} \tag{43}$$

where $\lambda_1 = -i\omega^{2/3} = \omega^{1/12} = \exp(\pi i/18)$ and $\lambda_2 = \lambda_1^*$ (cf equations (32)–(34)) and we denoted for simplicity $\tilde{A}_i \equiv \tilde{A}_i^{(1)}$. We dropped the subscript n appearing in the transformation (37) because for $n = 2$ one has $(XZ^k)^2 = (XZ^k)^\dagger$ for $k = 0, 1, 2$ and $\tilde{A}_i^{(2)} = \tilde{A}_i^\dagger$ (cf equation (39)); nevertheless, we need to take into account the case $n = 2$ when constructing the Bell inequality.

We then note that at the second site we also have three independent unitary observables Z , ZX and ZX^2 [note that $(ZX)^3 = (ZX^2)^3 = \mathbb{1}$], and therefore we can directly substitute

$$Z \rightarrow B_0, \quad ZX \rightarrow B_1, \quad ZX^2 \rightarrow B_2. \tag{44}$$

At the third site we have Z, Z^2 which represent a single measurement (cf section 2.1), and X which is independent of the other two. We thus substitute $Z^k \rightarrow C_0^k$ with $k = 1, 2$ and $X \rightarrow C_1$. Analogously, for the fourth party we have $Z \rightarrow D_0$ and $ZX \rightarrow D_1$.

Taking all the above substitutions into account we arrive at the following assignments

$$G_1 \rightarrow \langle \tilde{A}_0^{(1)} B_0 D_0 \rangle, \quad G_1 G_2 \rightarrow \langle \tilde{A}_1^{(1)} B_1 C_0 D_0 \rangle, \quad G_1 G_2^2 \rightarrow \langle \tilde{A}_2^{(1)} B_2 C_0^2 D_0 \rangle, \tag{45}$$

$$G_1 G_4 \rightarrow \langle \tilde{A}_1^{(1)} B_0 C_0^2 D_1 \rangle, \tag{46}$$

and for G_3 :

$$G_3 \rightarrow \langle B_0 C_1 D_0 \rangle. \tag{47}$$

Notice that the expectation values corresponding to $n = 2$ in the assignment (37) are simply complex conjugations of the above ones. By adding all the obtained expectation values, we finally obtain a Bell inequality of the form

$$\begin{aligned}
I_{\text{AME}} &:= \frac{1}{\sqrt{3}\lambda_1} [\langle (A_0 + A_1 + A_2) B_0 D_0 \rangle + \langle (A_0 + \omega^2 A_1 + \omega A_2) B_2 C_0^2 D_0 \rangle] \\
&+ \frac{1}{2\sqrt{3}\lambda_1\omega} [\langle (A_0 + \omega A_1 + \omega^2 A_2) B_1 C_0 D_0 \rangle + \langle (A_0 + \omega A_1 + \omega^2 A_2) B_0 C_0^2 D_1 \rangle] \\
&+ \langle B_0 C_1 D_0 \rangle + c.c. \leq \beta_{\text{AME}}^C,
\end{aligned} \tag{48}$$

where c.c. stands for the complex conjugation of all five terms and represents the expectation values obtained for the case $n = 2$ of the assignment (37); in particular, it makes the Bell expression real. Moreover, the second line comes with $1/2$ coefficient for reasons that will become clear later. The classical value in this case is

$$\beta_{\text{AME}}^C = 2 + 3(\omega^{-1/3} + \omega^{2/3} - \omega^{4/3}) = 7.638\ 16. \tag{49}$$

Let us prove that the maximal quantum violation of this inequality is $\beta_{\text{AME}}^Q = 8$. First, denoting by \mathcal{B}_{AME} a Bell operator constructed from I_{AME} , we can write the following sum-of-squares decomposition, which is inspired by the sum-of-squares decompositions found in [24]:

$$\begin{aligned}
8\mathbb{1} - \mathcal{B}_{\text{AME}} &= (\mathbb{1} - \tilde{A}_0 B_0 D_0)^\dagger (\mathbb{1} - \tilde{A}_0 B_0 D_0) + (\mathbb{1} - \tilde{A}_2 B_2 C_0^2 D_0)^\dagger (\mathbb{1} - \tilde{A}_2 B_2 C_0^2 D_0) \\
&+ \frac{1}{2} (\mathbb{1} - \tilde{A}_1 B_1 C_0 D_0)^\dagger (\mathbb{1} - \tilde{A}_1 B_1 C_0 D_0) + \frac{1}{2} (\mathbb{1} - \tilde{A}_1 B_0 C_0^2 D_1)^\dagger (\mathbb{1} - \tilde{A}_1 B_0 C_0^2 D_1) \\
&+ (\mathbb{1} - B_0 C_1 D_0)^\dagger (\mathbb{1} - B_0 C_1 D_0),
\end{aligned} \tag{50}$$

where A_x, B_y , etc are arbitrary three-outcome unitary observables. To prove that this decomposition holds true one simply expands its right-hand side and uses the property (cf equation (40)), which in the particular case $d = 3$ reads,

$$\tilde{A}_0^\dagger \tilde{A}_0 + \tilde{A}_1^\dagger \tilde{A}_1 + \tilde{A}_2^\dagger \tilde{A}_2 = 3\mathbb{1}. \tag{51}$$

Now it becomes clear why the second line of I_{AME} comes with $1/2$.

From this decomposition we immediately conclude that $8\mathbb{1} - \mathcal{B}_{\text{AME}} \geq 0$ for any choice of the local observables, which implies that also for any state $|\psi\rangle$, $\langle\psi|\mathcal{B}_{\text{AME}}|\psi\rangle \leq 8$. To show that this bound is tight it suffices to provide a quantum realisation achieving it. Such a realisation can be constructed by inverting the transformation in equations (43) and (44), that is, by taking

$$A_x = \frac{\lambda_1}{\sqrt{3}} \sum_{k=0}^2 \omega^{xk} \omega^{k(k+1)} O_k \quad (k = 0, 1, 2), \quad (52)$$

and $B_y = ZX^y$ with $y = 0, 1, 2$, $C_0 = Z$ and $C_1 = X$, and $D_w = ZX^w$ with $w = 0, 1$, we can bring the Bell operator \mathcal{B}_{AME} to

$$\mathcal{B}_{\text{AME}} = G_1 + G_1 G_2^2 + \frac{1}{2}(G_1 G_2 + G_1 G_4) + G_3 + h.c., \quad (53)$$

which is simply a sum of the stabilising operators of $|\text{AME}(4, 3)\rangle$. As a result, the latter achieves the maximal quantum value of the Bell inequality (48).

Example 2 (Two-qudit maximally entangled state). Let us then consider the case of arbitrary prime d and construct Bell inequalities for the simplest graph state which is the maximally entangled state (18) stabilised by the two generators given in equation (19).

Since we are now concerned with the bipartite scenario we can denote the observables measured by the parties by A_x and B_y ; the numbers of observables on both sites will be specified later. As already explained, to construct Bell inequalities we cannot simply use the replacement (25), we rather need to employ the one in equation (37). Let us moreover assume that we implement this transformation at Alice's site.

To be able to apply the above assignments, we need to consider a larger set of stabilising operators which apart from X and Z^k operators contain also $(XZ^k)^n$ with $k = 0, \dots, d-1$ and $n = 1, \dots, d-1$. To construct such a set one can for instance take the following products of G'_i given in equation (19):

$$G'_1 (G'_2)^k = XZ^k \otimes XZ^{-k} \quad (k = 0, 1, \dots, d-1). \quad (54)$$

However, to take into account all the outcomes of the measurements performed by both parties we need to also include the powers of the above stabilising operators (cf section 2.1) which leads us to the following $d(d-1)$ stabilising operators of $|\psi_d^+\rangle$:

$$\mathcal{G}_k^n := [G'_1 (G'_2)^k]^n = (XZ^k)^n \otimes (XZ^{-k})^n \quad (k = 0, \dots, d-1; n = 1, \dots, d-1). \quad (55)$$

We can now construct Bell inequalities maximally violated by the two-qudit maximally entangled states. Precisely, to each of the stabilising operators \mathcal{G}_k^n we associate an expectation value in which the particular matrices appearing at the first site are replaced by the combinations (37) of the observables A_x ,

$$(XZ^k)^n \rightarrow \tilde{A}_k^{(n)}, \quad (56)$$

whereas at the second site we substitute directly

$$(XZ^{-k})^n \rightarrow B_k^n. \quad (57)$$

In other words, we associate

$$\mathcal{G}_k^n \rightarrow \langle \tilde{A}_k^{(n)} B_k^n \rangle \quad (58)$$

with $k = 0, 1, 2$ and $n = 1, 2$.

Adding then all the obtained expectation values and exploiting the fact that $\lambda_n^{-1} = \lambda_n^*$, we finally arrive at Bell inequalities derived previously in [24]:

$$\begin{aligned} I_{\text{max}} &:= \sum_{n=1}^{d-1} \sum_{k=0}^{d-1} \langle \tilde{A}_k^{(n)} B_k^n \rangle \\ &= \frac{1}{\sqrt{d}} \sum_{n=1}^{d-1} \lambda_n^* \sum_{x,y=0}^{d-1} \omega^{-nxy} \langle A_x^n B_y^n \rangle \leq \beta_{\text{max}}^C, \end{aligned} \quad (59)$$

Table 1. Maximal classical values of the Bell expression I_{\max} given in equation (59) for $d = 3, 5, 7$. For comparison we also present the maximal quantum values.

d	β_L	β_Q	β_Q/β_L
3	$6 \cos(\pi/9)$	6	1.064
5	$4(2 + \sqrt{5})$	20	1.1803
7	$\simeq 33.3494$	42	1.2594

where β_{\max}^C stands for the maximal classical value of I_{\max} . It is in general difficult to compute β_{\max}^C analytically, however, for the lowest values of $d = 3, 5, 7$ it was found numerically in [24]; for completeness we listed these values in table 1.

On the other hand, these Bell inequalities are designed so that their maximal quantum value can be determined straightforwardly. Let us formulate and prove the following fact.

Fact 1. *The maximal quantum value of the Bell expressions $I_{\max}^{(d)}$ is $\beta_{\max}^Q = d(d-1)$.*

Proof. The proof is straightforward and consists of two steps. First, we denote by

$$\mathcal{B}_{\max} = \frac{1}{\sqrt{d}} \sum_{n=1}^{d-1} \frac{1}{\lambda_n} \sum_{x,y=0}^{d-1} \omega^{-nxy} A_x^n \otimes B_y^n \quad (60)$$

a Bell operator associated to the expression $I_{\max}^{(d)}$, where A_x and B_y are arbitrary d -outcome unitary observables. Second, one uses equation (40) as well as the fact that the Bell operator is Hermitian to observe that the following sum-of-squares decomposition holds true

$$d(d-1)\mathbb{1} - \mathcal{B}_{\max} = \frac{1}{2} \sum_{n=1}^{d-1} \sum_{y=0}^{d-1} \left(\mathbb{1} - \tilde{A}_y^{(n)} \otimes B_y^n \right)^\dagger \left(\mathbb{1} - \tilde{A}_y^{(n)} \otimes B_y^n \right). \quad (61)$$

Consequently, $d(d-1)\mathbb{1} - \mathcal{B}_{\max}$ is a positive semi-definite operator for any choice of local observables, and thus $\beta_{\max}^{(d)} \leq d(d-1)$. To prove that this inequality is tight we can construct a quantum realisation for which $I_{\max}^{(d)} = d(d-1)$. Precisely, we notice that for the following choice of observables for Alice and Bob (cf equation (38)),

$$A_x^n = \frac{\lambda_n}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{n x k} \omega^{n k(k+1)} (XZ^k)^n, \quad B_y^n = (XZ^{-k})^n \quad (62)$$

the Bell operator \mathcal{B}_{\max} simply becomes a sum of the stabilising operators of $|\psi_d^+\rangle$,

$$\mathcal{B}_{\max} = \sum_{n=1}^{d-1} \sum_{k=0}^{d-1} [G_1'(G_2')^k]^n, \quad (63)$$

meaning that $\langle \psi_d^+ | \mathcal{B}_{\max} | \psi_d^+ \rangle = d(d-1)$. As a result $\beta_{\max}^{(d)} = d(d-1)$, which completes the proof. \square

3.4. General construction

We are now ready to provide our general construction of Bell inequalities for arbitrary graph states. Let us first set the notation.

Consider a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{R}, d)$ and choose two of its vertices that are connected. Without any loss of generality we can label them by 1 and 2. Let then \mathcal{N}_1 and N_1 be respectively the neighbourhood of the first vertex, i.e. the set of all vertices that are connected to it, and its cardinality. Clearly, we can relabel all the other neighbours of vertex 1 by $j \in \mathcal{N}_1 \setminus \{2\} \equiv \{3, \dots, N_1 + 1\}$. We finally label the remaining vertices that are not connected to the first vertex as $l \in \mathcal{V} \setminus \{1, \mathcal{N}_1\} \equiv \{N_1 + 2, \dots, N\}$. The generators corresponding to the graph \mathcal{G} are denoted G_i (see equation (14) for the definition thereof), whereas the graph state stabilised by them by $|G\rangle$.

Let us then define the Bell scenario. It will be beneficial for our construction to slightly modify the way we denote the observers and the observables they measure. Precisely, the observables measured by the first two parties are denoted by A_x and B_y with $x, y = 0, \dots, d-1$, respectively; notice that both them can choose among d different settings. Then, the other observers connected to the first party A measure three

observables which we denote $C_z^{(i)}$ with $z = 0, 1, 2$ and $i \in \mathcal{N}_1 \setminus \{2\}$. The remaining observers (that do not belong to \mathcal{N}_1) have only two observables at their disposal, denoted $D_0^{(i)}, D_1^{(i)}$ where $i \in \{N_1 + 2, \dots, N\}$.

Before providing our construction in detail let us first present a short overview of it. Analogously to the examples presented above, for a given graph \mathcal{G} and the corresponding graph state $|\psi_G\rangle$, we first construct a sufficiently large set of stabilising operators (together with their matrix powers) obtained from the generators G_i . Then, to each of these stabilising operators we associate an expectation value in which the local matrices are replaced by arbitrary observables of their combinations; in fact, at the first site we implement the replacement rule (37), whereas at the remaining sites the operators are directly replaced by the observables. The motivation to use (37) is that it allows to obtain nontrivial Bell inequalities for which the quantum and classical values differ (see [20, 24]). Then, a suitable combination of the obtained expectation values gives rise to a Bell expression (cf equation (84)) whose maximal value can be analytically determined by constructing a suitable sum-of-squares decomposition, as shown in theorem 2 below. Importantly, the above replacement rule can be reversed in the sense that by choosing suitable observables for each of the observers—in particular the first observer measures the observables defined in equation (38)—one can bring the corresponding Bell operator to a sum of the stabilising operators of the given graph state (cf equation (97)), which allows one to show that the graph state $|\psi_G\rangle$ achieves the maximal quantum value of the given Bell expression.

Let us now present our construction in more detail. To derive a Bell inequality tailored to the graph state $|\mathcal{G}\rangle$ we begin by rewriting the stabilising operators G_i corresponding to \mathcal{G} by explicitly presenting operators acting on the first two sites as well as on the neighbourhood \mathcal{N}_1 . The first two stabilising operators read

$$G_1 = X_1 \otimes Z_2^{r_{1,2}} \otimes \bigotimes_{m \in \mathcal{N}_1 \setminus \{2\}} Z_m^{r_{1,m}} \quad (64)$$

and

$$G_2 = Z_1^{r_{1,2}} \otimes X_2 \otimes \bigotimes_{m \in \mathcal{N}_1 \setminus \{2\}} Z_m^{r_{2,m}} \otimes \bigotimes_{m=N_1+2}^N Z_m^{r_{2,m}}. \quad (65)$$

Then, those associated to the other vertices belonging to \mathcal{N}_1 are given by

$$G_i = Z_1^{r_{1,i}} \otimes Z_2^{r_{2,i}} \otimes X_i \otimes \bigotimes_{m \in \mathcal{N}_1 \setminus \{2,i\}} Z_m^{r_{i,m}} \otimes \bigotimes_{m=N_1+2}^N Z_m^{r_{i,m}}, \quad (66)$$

where $j = 3, \dots, N_1$, whereas the remaining G_i 's for $i \in \{N_1 + 2, \dots, N\}$ are of the following form

$$G_i = \mathbb{1}_1 \otimes Z_2^{r_{2,i}} \otimes \bigotimes_{m \in \mathcal{N}_1 \setminus \{2\}} Z_m^{r_{i,m}} \otimes X_i \otimes \bigotimes_{m \in \{N_1+2, \dots, N\} \setminus \{i\}} Z_m^{r_{i,m}}. \quad (67)$$

It is worth adding here that since by assumption the first two vertices are connected, $r_{1,2} \neq 0$. Moreover, G_1 acts trivially on all sites that are outside $\mathcal{N}_1 \cup \{1\}$.

Given the stabilising operators, let us then follow the procedure outline already in the previous examples. We begin by constructing a suitable set of stabilising operators. First, to create at the first site the operators XZ^k required for the assignment (37), we consider products $G_1 G_2^k$ with $k = 0, \dots, d-1$. This set, however, does not uniquely define the graph state $|\mathcal{G}\rangle$ as it lacks the other generators. To include them we first notice that any G_i with $i \in \mathcal{N}_1 \setminus \{2\}$ contains the Z operator or its power at the first position and therefore we take their products with G_1 , that is, $G_1 G_i$ with $i \in \mathcal{N}_1 \setminus \{2\}$, again to obtain XZ^k at the first site. On the other hand, the remaining generators G_i for $i \in \{N_1 + 2, \dots, N\}$ have the identity at the first position and therefore we directly add them to the set.

Thus, the total list of the stabilizing operators that we use to construct a Bell inequality is

$$\begin{aligned} \mathcal{G}_{1,k}^n &:= (G_1 G_2^k)^n \quad (k = 0, \dots, d-1), \\ \mathcal{G}_{2,k}^n &:= (G_1 G_k)^n \quad (k = 3, \dots, N_1 + 1), \\ \mathcal{G}_{3,k}^n &:= G_k^n \quad (k = N_1 + 2, \dots, N), \end{aligned} \quad (68)$$

where we have added powers to include all outcomes in the Bell scenario. Let us now write these operators explicitly

$$\mathcal{G}_{1,k}^n = (XZ^{kr_{1,2}})_1^n \otimes (Z^{r_{1,2}} X^k)_2^n \otimes \bigotimes_{m \in \mathcal{N}_1 \setminus \{2\}} Z_m^{r_{1,m} + kr_{2,m}} \otimes \bigotimes_{m \in \{N_1+2, \dots, N\}} Z_m^{nkr_{2,m}} \quad (69)$$

for $k = 0, \dots, d-1$,

$$\mathcal{G}_{2,k}^n = (XZ^{r_{1,k}})_1^n \otimes Z_2^{n(r_{1,2}+r_{2,k})} \otimes (Z^{r_{1,k}}X)_k^n \otimes \bigotimes_{m \in \mathcal{N}_1 \setminus \{2,k\}} Z_m^{n(r_{1,m}+r_{k,m})} \otimes \bigotimes_{m \in \{N_1+2, \dots, N\}} Z_m^{nr_{k,m}} \quad (70)$$

for $k = 3, \dots, N_1 + 2$, and

$$\mathcal{G}_{3,k}^n = \mathbb{1}_1 \otimes Z_2^{nr_{2,k}} \otimes \bigotimes_{m \in \mathcal{N}_1 \setminus \{2\}} Z_m^{nr_{k,m}} \otimes X_k^n \otimes \bigotimes_{m \in \{N_1+2, \dots, N\} \setminus \{k\}} Z_m^{nr_{k,m}} \quad (71)$$

for $k \in \{N_1 + 2, \dots, N\}$.

We associate to each of these stabilising operators an expectation value in which the local operators are replaced by d -outcome observables or combinations thereof. Let us begin with the first site where we have $(XZ^{kr_{1,2}})^n$ with $k = 0, \dots, d-1$, $XZ^{r_{1,i}}$ with $i = 3, \dots, N_1$ and the identity. It is important to notice here that due to the fact that d is a prime number, for any $r_{1,2} \neq 0$, $kr_{1,2}$ spans the whole set $\{0, \dots, d-1\}$ for $k = 0, \dots, d-1$; in other words, the function $f(k) = kr_{1,2}$ defined on the set $\{0, \dots, d-1\}$ is a one-to-one function. Thus, $XZ^{kr_{1,2}}$ contains all the d different matrices appearing in the transformation (37). We thus substitute

$$(XZ^{kr_{1,2}})^n \rightarrow \tilde{A}_{kr_{1,2}}^{(n)} := \frac{\omega^{-nkr_{1,2}(kr_{1,2}+1)}}{\sqrt{d}\lambda_n} \sum_{x=0}^{d-1} \omega^{-nkr_{1,2}x} A_x^n. \quad (72)$$

Analogously, we substitute

$$(XZ^{r_{1,i}})^n \rightarrow \tilde{A}_{r_{1,i}}^{(n)} := \frac{\omega^{-nr_{1,i}(kr_{1,i}+1)}}{\sqrt{d}\lambda_n} \sum_{x=0}^{d-1} \omega^{-nr_{1,i}x} A_x^n \quad (73)$$

for $i = 3, \dots, N_1 + 1$; in both cases $n = 1, \dots, d-1$.

Let us then move to the second site. The matrices appearing there are $Z^{r_{1,2}}X^k$ with $k = 0, \dots, d-1$ and $Z^{n(r_{1,2}+r_{2,i})}$ with $i = 3, \dots, N_1 + 1$. Since for any $r_{1,2}$ the former are all proper observables in our scenario, that is, they are unitary and their spectra belong to $\{1, \omega^1, \dots, \omega^{d-1}\}$, we can directly substitute them by observables B_k . Specifically, for $k = 0$ we assign

$$Z^n \rightarrow B_0^n \quad (74)$$

which implies in particular that

$$Z^{nr_{1,2}} \rightarrow B_0^{nr_{1,2}}, \quad (75)$$

and for the remaining $k = 1, \dots, d-1$,

$$(Z^{r_{1,2}}X^k)^n \rightarrow B_k^n. \quad (76)$$

We distinguish the case $k = 0$ to simplify the assignment of observables to the other set of matrices $Z^{n(r_{1,2}+r_{2,i})}$ with $i = 3, \dots, N_1 + 1$. These are simply powers of Z and thus we associate with them a single observable B_0 ; precisely,

$$Z^{n(r_{1,2}+r_{2,i})} \rightarrow B_0^{n(r_{1,2}+r_{2,i})}. \quad (77)$$

Let us now consider all sites from $\mathcal{N}_1 \setminus \{2\}$. From equations (69), (70) and (71) it follows that the operators appearing there are $Z^{r_{1,i}}X$ with $i = 3, \dots, N_1 + 1$ and powers of Z , and thus we can make the following replacements

$$Z \rightarrow C_0^{(i)} \quad \text{and} \quad Z^{r_{1,i}}X \rightarrow C_1^{(i)} \quad (78)$$

for any $i = 3, \dots, N_1$. Finally, for the remaining sites we have simply the X operator at various sites and powers of Z . Thus, for any $i = N_1 + 2, \dots, N$,

$$Z \rightarrow D_0^{(i)} \quad \text{and} \quad X \rightarrow D_1^{(i)}. \quad (79)$$

Collecting all these substitutions together we have

$$\mathcal{G}_{1,0}^n \rightarrow \tilde{\mathcal{G}}_{1,0}^{(n)} := \tilde{A}_0^{(n)} \otimes B_0^{nr_{1,2}} \otimes \bigotimes_{i=3}^{N_1+1} [C_0^{(i)}]^{nr_{1,i}} \quad (80)$$

and

$$\mathcal{G}_{1,k}^n \rightarrow \tilde{\mathcal{G}}_{1,k}^{(n)} := \tilde{A}_{kr_{1,2}}^{(n)} \otimes B_k^n \otimes \bigotimes_{i=3}^{N_1+1} [C_0^{(i)}]^{n(r_{1,i}+kr_{2,i})} \otimes \bigotimes_{i=N_1+2}^N [D_0^{(i)}]^{nkr_{2,i}} \quad (81)$$

for $k = 1, \dots, d-1$. Then,

$$\mathcal{G}_{2,k}^n \rightarrow \tilde{\mathcal{G}}_{2,k}^{(n)} := \tilde{A}_{r_{1,k}}^{(n)} \otimes B_0^{n(r_{1,k}+r_{2,k})} \bigotimes_{i=3}^{k-1} [C_0^{(i)}]^{n(r_{1,i}+r_{k,i})} \otimes [C_1^{(k)}]^n \otimes \bigotimes_{i=k+1}^{N_1+1} [C_0^{(i)}]^{n(r_{1,i}+r_{k,i})} \bigotimes_{i=N_1+2}^N [D_0^{(i)}]^{nr_{k,i}} \quad (82)$$

with $k \in \{3, \dots, N_1+1\}$, and, finally,

$$\mathcal{G}_{3,k}^n \rightarrow \tilde{\mathcal{G}}_{3,k}^{(n)} := B_0^{nr_{2,k}} \bigotimes_{i=3}^{N_1+1} [C_0^{(i)}]^{nr_{k,i}} \bigotimes_{i=N_1+2}^{k-1} [D_0^{(i)}]^{nr_{k,i}} \otimes [D_1^{(k)}]^n \otimes \bigotimes_{i=k+1}^N [D_0^{(i)}]^{nr_{k,i}} \quad (83)$$

for $k \in \{N_1+2, \dots, N\}$.

Lastly, by taking a weighted sum of expectation values of the above operators, we arrive at the following class of Bell expressions for a given graph state:

$$I_{\mathcal{G}} := \sum_{n=1}^{d-1} \left[\langle \tilde{\mathcal{G}}_{1,0}^{(n)} \rangle + \sum_{k=1}^{d-1} c_{1,k} \langle \tilde{\mathcal{G}}_{1,k}^{(n)} \rangle + \sum_{k=3}^{N_1+1} c_{2,k} \langle \tilde{\mathcal{G}}_{2,k}^{(n)} \rangle + \sum_{k=N_1+2}^N \langle \tilde{\mathcal{G}}_{3,k}^{(n)} \rangle \right], \quad (84)$$

where $c_{i,k} > 0$ are some free parameters that satisfy

$$c_{1,k} + \sum_{\substack{j=3 \\ \{j:r_{1,j}=kr_{1,2}\}}}^{N_1+1} c_{2,j} = 1 \quad (85)$$

for each $k = 1, \dots, d-1$, where the second sum goes over all j such that for a fixed k , $r_{1,j} = kr_{1,2}$. As we will see below the conditions (85) are used for constructing sum-of-squares decompositions of the Bell operators corresponding to $I_{\mathcal{G}}$, which in turn are crucial for determining the maximal quantum values of $I_{\mathcal{G}}$. In fact, we can prove the following theorem.

Theorem 2. *The maximal quantum value of $I_{\mathcal{G}}$ is*

$$\beta_{\mathcal{G}}^Q = (d-1)(N-N_1+d-1). \quad (86)$$

Proof. To prove this statement let us consider a Bell operator corresponding to $I_{\mathcal{G}}$,

$$\mathcal{B}_{\mathcal{G}} = \sum_{n=1}^{d-1} \left[\tilde{\mathcal{G}}_{1,0}^{(n)} + \sum_{k=1}^{d-1} c_{1,k} \tilde{\mathcal{G}}_{1,k}^{(n)} + \sum_{k=3}^{N_1+1} c_{2,k} \tilde{\mathcal{G}}_{2,k}^{(n)} + \sum_{k=N_1+2}^N \tilde{\mathcal{G}}_{3,k}^{(n)} \right], \quad (87)$$

where $\tilde{\mathcal{G}}_{i,k}^{(n)}$ are defined in equations (80)–(83). We show that $\mathcal{B}_{\mathcal{G}}$ admits the following sum-of-squares decomposition

$$\begin{aligned} \mathcal{B}_{\mathcal{G}} &= (d-1)(N-N_1+d-1)\mathbb{1} \\ &\quad - \frac{1}{2} \sum_{n=1}^{d-1} \left[\left(\mathbb{1} - \tilde{\mathcal{G}}_{1,0}^{(n)} \right)^{\dagger} \left(\mathbb{1} - \tilde{\mathcal{G}}_{1,0}^{(n)} \right) + \sum_{k=1}^{d-1} c_{1,k} \left(\mathbb{1} - \tilde{\mathcal{G}}_{1,k}^{(n)} \right)^{\dagger} \left(\mathbb{1} - \tilde{\mathcal{G}}_{1,k}^{(n)} \right) \right. \\ &\quad \left. + \sum_{k=3}^{N_1+1} c_{2,k} \left(\mathbb{1} - \tilde{\mathcal{G}}_{2,k}^{(n)} \right)^{\dagger} \left(\mathbb{1} - \tilde{\mathcal{G}}_{2,k}^{(n)} \right) + \sum_{k=N_1+2}^N \left(\mathbb{1} - \tilde{\mathcal{G}}_{3,k}^{(n)} \right)^{\dagger} \left(\mathbb{1} - \tilde{\mathcal{G}}_{3,k}^{(n)} \right) \right]. \quad (88) \end{aligned}$$

To verify that this decomposition holds true let us expand the expression appearing in the square brackets for a particular n ,

$$\begin{aligned} & \left(1 + \sum_{k=1}^{d-1} c_{1,k} + \sum_{k=3}^{N_1+1} c_{2,k} + N - N_1 - 1 \right) \mathbb{1} - \mathcal{B}_{\mathcal{G}}^{(n)} - [\mathcal{B}_{\mathcal{G}}^{(n)}]^{\dagger} + (\tilde{\mathcal{G}}_{1,0}^{(n)})^{\dagger} \tilde{\mathcal{G}}_{1,0}^{(n)} \\ & + \sum_{k=1}^{d-1} c_{1,k} (\tilde{\mathcal{G}}_{1,k}^{(n)})^{\dagger} \tilde{\mathcal{G}}_{1,k}^{(n)} + \sum_{k=3}^{N_1+1} c_{2,k} (\tilde{\mathcal{G}}_{2,k}^{(n)})^{\dagger} \tilde{\mathcal{G}}_{2,k}^{(n)} + \sum_{k=N_1+2}^N (\tilde{\mathcal{G}}_{3,k}^{(n)})^{\dagger} \tilde{\mathcal{G}}_{3,k}^{(n)}, \end{aligned} \quad (89)$$

where $\mathcal{B}_{\mathcal{G}}^{(n)}$ is a part of the Bell operator corresponding to a particular n , that is,

$$\mathcal{B}_{\mathcal{G}}^{(n)} = \tilde{\mathcal{G}}_{1,0}^{(n)} + \sum_{k=1}^{d-1} c_{1,k} \tilde{\mathcal{G}}_{1,k}^{(n)} + \sum_{k=3}^{N_1+1} c_{2,k} \tilde{\mathcal{G}}_{2,k}^{(n)} + \sum_{k=N_1+2}^N c_{3,k} \tilde{\mathcal{G}}_{3,k}^{(n)}. \quad (90)$$

We now notice that by summing all the conditions (85) one can deduce that

$$\sum_{k=1}^{d-1} c_{1,k} + \sum_{k=3}^{N_1+1} c_{2,k} = d - 1, \quad (91)$$

which implies that the coefficient in front of the identity simplifies to $d + N - N_1 - 1$. Using the definitions of $\tilde{\mathcal{G}}_{i,k}^{(n)}$ one then has that

$$\begin{aligned} & (\tilde{\mathcal{G}}_{1,0}^{(n)})^{\dagger} \tilde{\mathcal{G}}_{1,0}^{(n)} + \sum_{k=1}^{d-1} c_{1,k} (\tilde{\mathcal{G}}_{1,k}^{(n)})^{\dagger} \tilde{\mathcal{G}}_{1,k}^{(n)} + \sum_{k=3}^{N_1+1} c_{2,k} (\tilde{\mathcal{G}}_{2,k}^{(n)})^{\dagger} \tilde{\mathcal{G}}_{2,k}^{(n)} + \sum_{k=N_1+2}^N (\tilde{\mathcal{G}}_{3,k}^{(n)})^{\dagger} \tilde{\mathcal{G}}_{3,k}^{(n)} \\ & = (\tilde{A}_0^{(n)})^{\dagger} \tilde{A}_0^{(n)} + \sum_{k=1}^{d-1} c_{1,k} (\tilde{A}_{kr_{1,2}}^{(n)})^{\dagger} \tilde{A}_{kr_{1,2}}^{(n)} + \sum_{k=3}^{N_1+1} c_{2,k} (\tilde{A}_{r_{1,k}}^{(n)})^{\dagger} \tilde{A}_{r_{1,k}}^{(n)} + (N - N_1 - 1) \mathbb{1} \\ & = \sum_{k=0}^{d-1} (\tilde{A}_k^{(n)})^{\dagger} \tilde{A}_k^{(n)} + (N - N_1 - 1) \mathbb{1} = (d + N - N_1 - 1) \mathbb{1}, \end{aligned} \quad (92)$$

where the second line follows from the fact that apart from the first position all the local operators in $\tilde{\mathcal{G}}_{i,k}^{(n)}$ are unitary (notice also that $\tilde{\mathcal{G}}_{3,k}^{(n)}$ have the identity at the first position), whereas the second line stems from the conditions (40) and (85). All this allows us to rewrite (89) simply as $2(d + N - N_1 - 1) \mathbb{1} - \mathcal{B}_{\mathcal{G}}^{(n)} - \mathcal{B}_{\mathcal{G}}^{(n)\dagger}$. Taking finally the sum of these terms over $n = 1, \dots, d - 1$ we arrive at the decomposition (88), which completes the first part of the proof.

From the decomposition (88) one directly infers that $(d - 1)(d + N - N_1 - 1) \mathbb{1} - \mathcal{B}_{\mathcal{G}}$ is a positive semi-definite operator for any choice of the local observables, which is equivalent to say that for any Bell operator $\mathcal{B}_{\mathcal{G}}$ corresponding to $I_{\mathcal{G}}$ and any pure state $|\psi\rangle$, the following inequality is satisfied

$$\langle \psi | \mathcal{B}_{\mathcal{G}} | \psi \rangle \leq (d - 1)(d + N - N_1 - 1). \quad (93)$$

To show that this inequality is tight, and at the same time complete the proof, let us provide a particular quantum realisation that achieves it. To this end, we can invert the transformation we used to construct $I_{\mathcal{G}}$. Precisely, we let the first party measure d observables A_k with $k = 0, \dots, d - 1$ which are defined in equation (38); for them $\tilde{A}_k^{(n)} = (XZ^k)^n$. The remaining parties measure

$$B_0^n = Z^n, \quad B_k^n = (Z^{r_{1,2}} X^k)^n \quad (k = 0, \dots, d - 1) \quad (94)$$

$$C_0^{(i)} = Z, \quad C_1^{(i)} = Z^{r_{1,i}} X \quad (95)$$

for $i = 3, \dots, N_1 + 1$, and, finally,

$$D_0^{(i)} = Z, \quad D_1^{(i)} = X \quad (96)$$

for $i = N_1 + 2, \dots, N$.

It is not difficult to see that for this choice of quantum observables the Bell operator reduces to a combination of the stabilising operators of the given graph state $|G\rangle$, that is,

$$\mathcal{B}_G = \sum_{n=1}^{d-1} \left[G_1^n + \sum_{k=1}^{d-1} c_{1,k} (G_1 G_2^k)^n + \sum_{k=3}^{N_1+1} c_{2,k} (G_1 G_k)^n + \sum_{k=N_1+2}^N G_k^n \right]. \quad (97)$$

Owing to the conditions (85) as well as (91), one finds that

$$\langle G | \mathcal{B}_G | G \rangle = (d-1)(N - N_1 + d - 1), \quad (98)$$

which is what we aimed to prove. \square

We have thus obtained a family of Bell expressions whose maximal quantum values are achieved by graph states of arbitrary prime local dimension. To turn them into nontrivial Bell inequalities one still needs to determine their maximal classical values which is in general a hard task. For the simplest cases such as Bell inequalities for the AME(4,3) state or those tailored to the maximally entangled state of two qudits for low d 's, the classical bounds can be determined numerically (cf equation (49) and table 1). On the other hand, in the next section we show that our inequalities allow to self-test the graph states of local dimension three, and thus for all of them the classical bound is strictly lower than the Tsirelson's bound. It is also worth mentioning that the ratio between the maximal quantum and classical values will certainly depend on the choice of vertices 1 and 2, in particular on the number of neighbours of the first vertex N_1 because this number appears in the formula for β_Q (86).

Let us finally mention that our inequalities are scalable in the sense that the number of expectation values they are constructed from scales linearly with N . Indeed, it follows from equation (84) that the number of expectation values in I_G is

$$(d-1)[N + (N_1 + d)(d-1)] \quad (99)$$

which in the worst case $N_1 = N - 1$ reduces to $(d-1)[Nd + (d-1)^2]$. This number can still be lowered twice because the expectation values in I_G for $n = \lceil d/2 \rceil, \dots, d-1$ are complex conjugations of those for $n = 1, \dots, \lfloor d/2 \rfloor$. Another possibility for lowering its number is to choose as the first vertex the one with the lowest neighbourhood. While it is an interesting question whether it is possible to design another construction which requires measuring even less expectation values, it seems that the linear scaling in N is the best one can hope for.

4. Self-testing of qutrit graph states

Here we show our second main result: we demonstrate that our Bell inequalities can be used to self-test arbitrary graph states of local dimension $d = 3$. In this particular case the general Bell expression (84) can be written as

$$I_G := \langle \tilde{\mathcal{G}}_{1,0}^{(n)} \rangle + \sum_{k=1}^{d-1} c_{1,k} \langle \tilde{\mathcal{G}}_{1,k}^{(n)} \rangle + \sum_{k=3}^{N_1+1} c_{2,k} \langle \tilde{\mathcal{G}}_{2,k}^{(n)} \rangle + \sum_{k=N_1+2}^N \langle \tilde{\mathcal{G}}_{3,k}^{(n)} \rangle + \text{c.c.}, \quad (100)$$

or explicitly as,

$$\begin{aligned} I_G := & \left\langle \tilde{A}_0 B_0^{r_{1,2}} \prod_{i=3}^{N_1+1} [C_0^{(i)}]^{r_{1,i}} \right\rangle \\ & + \sum_{k=1}^2 c_{1,k} \left\langle \tilde{A}_{kr_{1,2}} B_k \prod_{i=3}^{N_1+1} [C_0^{(i)}]^{r_{1,i} + kr_{2,i}} \prod_{i=N_1+2}^N [D_0^{(i)}]^{kr_{2,i}} \right\rangle \\ & + \sum_{k=3}^{N_1+1} c_{2,k} \left\langle \tilde{A}_{r_{1,k}} B_0^{r_{1,k} + r_{2,k}} \prod_{i=3}^{k-1} [C_0^{(i)}]^{r_{1,i} + r_{k,i}} C_1^{(k)} \prod_{i=k+1}^{N_1+1} [C_0^{(i)}]^{r_{1,i} + r_{k,i}} \prod_{i=N_1+2}^N [D_0^{(i)}]^{r_{k,i}} \right\rangle \\ & + \sum_{k=N_1+2}^N \left\langle B_0^{r_{2,k}} \prod_{i=3}^{N_1+1} [C_0^{(i)}]^{r_{k,i}} \prod_{i=N_1+2}^{k-1} [D_0^{(i)}]^{r_{k,i}} D_1^{(k)} \prod_{i=k+1}^N [D_0^{(i)}]^{r_{k,i}} \right\rangle + \text{c.c.}, \end{aligned} \quad (101)$$

where c.c. stands for the complex conjugation and represents the $n = 2$ term in equation (84), whereas the coefficients $c_{1,k}$ and $c_{2,k}$ satisfy the condition (85).

Let us now prove that maximal violation of I_G can be used to self-test the corresponding graph state according to definition 1. To this aim, we state the following theorem.

Theorem 3. Consider a connected graph G and assume that the maximal quantum value of the corresponding Bell expression I_G is achieved by a pure state $|\psi\rangle \in \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_N$ and observables A_x, B_y , etc acting on the local Hilbert spaces \mathcal{H}_i . Then, each Hilbert space \mathcal{H}_i decomposes as $\mathcal{H}_i = \mathbb{C}^3 \otimes \mathcal{H}'_i$ and there exist local unitary operators U_i with $i = 1, \dots, N$ such that

$$(U_1 \otimes \dots \otimes U_N)|\psi\rangle = |\psi_G\rangle \otimes |\text{aux}\rangle \quad (102)$$

with $|\text{aux}\rangle$ being some state from the auxiliary Hilbert space $\mathcal{H}'_1 \otimes \dots \otimes \mathcal{H}'_N$.

Before we present our proof let us mention that it follows a similar reasoning to the proof of self-testing of N -qubit graph states in [20], but since we deal here with qutrits it also makes a use of one of the results of [24], which for completeness we state in appendix B as fact 5.

Proof. Let us first notice that it is convenient to assume that the local reduced density matrices of the state $|\psi\rangle$ are full rank; otherwise we are able to characterize the observables only on the supports of these reduced density matrices. Moreover, we assume for simplicity that $r_{1,2} = 1$; recall that by construction $r_{1,2} \neq 0$. The proof for the other case of $r_{1,2} = 2$ goes along the same lines.

The sum-of-squares decomposition (88) implies the following relations for the state and observables that achieve the maximal quantum value of the Bell expression I_G ,

$$\tilde{\mathcal{G}}_{1,k}^{(n)}|\psi\rangle = |\psi\rangle \quad (103)$$

for $k = 0, 1, 2$,

$$\tilde{\mathcal{G}}_{2,k}^{(n)}|\psi\rangle = |\psi\rangle \quad (104)$$

for $k = 3, \dots, N_1 + 1$, and

$$\tilde{\mathcal{G}}_{3,k}^{(n)}|\psi\rangle = |\psi\rangle \quad (105)$$

for $k = N_1 + 2, \dots, N$.

Before we employ the above relations in order to prove our self-testing statement let us recall that $\tilde{A}_x^{(n)}$ ($x = 0, 1, 2$) are combinations of the first party's observables and are not unitary in general; still, they satisfy $\tilde{A}_x^{(2)} = \tilde{A}_x^{(1)\dagger}$. At the same time $B_y, C_z^{(i)}$, and $D_w^{(i)}$ are all unitary observables which in the particular case $d = 3$ satisfy $B_y^2 = B_y^\dagger$ etc. This implies that $\tilde{\mathcal{G}}_{i,k}^{(2)} = \tilde{\mathcal{G}}_{i,k}^{(1)\dagger}$.

The main technical step we need is to identify at each site two unitary observables whose anticommutator is unitary. This allows us to make use of fact 5 and corollary 4 (see appendix B) to define local unitary operators that map the two unknown observables to the qutrit ones. For parties having three measurement choices, the remaining observable will be directly mapped to other qutrit operators thanks to anticommutation relations that can be inferred from the sum-of-squares decompositions.

Our proof is quite technical and long and therefore to make it easier to follow we divide it into a few steps. In the first four we characterize every party's observables that give rise to the maximal quantum violation of the inequality, while in the last one we prove the self-testing statement for the state.

Step 1. (A_x observables). Let us first determine the form of the first party's observables A_x . To this end, we concentrate on conditions (103) which for $n = 1$ and $r_{1,2} = 1$ can be rewritten as

$$\begin{aligned} \tilde{A}_0 \otimes B_0 \otimes \bar{C}_1 |\psi\rangle &= |\psi\rangle, \\ \tilde{A}_1 \otimes B_1 \otimes \bar{C}_1 \bar{C}_2 \bar{D} |\psi\rangle &= |\psi\rangle, \\ \tilde{A}_2 \otimes B_2 \otimes \bar{C}_1 \bar{C}_2^\dagger \otimes \bar{D}^\dagger |\psi\rangle &= |\psi\rangle, \end{aligned} \quad (106)$$

where \bar{C}_i and \bar{D} are short-hand notations for

$$\bar{C}_i = \bigotimes_{m=3}^{N_1+1} \left[C_0^{(m)} \right]^{r_{i,m}}, \quad \bar{D} = \bigotimes_{m=N_1+2}^N \left[D_0^{(m)} \right]^{r_{2,m}}, \quad (107)$$

where $i = 1, 2$, and, finally,

$$\tilde{A}_k \equiv \tilde{A}_k^{(1)} = \frac{\omega^{-k(k+1)}}{\sqrt{3} \lambda_1} \sum_{t=0}^2 \omega^{-tk} A_t. \quad (108)$$

Recall that in the case $d = 3$, $\tilde{A}_k^{(2)} = \tilde{A}_k^{(1)\dagger}$. Moreover, since $\tilde{G}_{i,k}^{(2)} = \tilde{G}_{i,k}^{(1)\dagger}$, equation (103) for $n = 2$ gives another set of conditions, similar to (106) but with all local operators being Hermitian-conjugated. By the very definition, B_i , \bar{C}_i and \bar{D} are unitary and satisfy $B_i^3 = \bar{C}_i^3 = \bar{D}^3 = \mathbb{1}$.

The above equations contain all three operators \tilde{A}_i ($i = 0, 1, 2$). Let us then concentrate on the first condition in (106) and use the fact that B_0 and \bar{C}_1 are unitary to rewrite it as

$$\tilde{A}_0|\psi\rangle = B_0^\dagger \otimes \bar{C}_1^\dagger |\psi\rangle, \quad (109)$$

which, taking into account that $B_0^3 = \mathbb{1}$ as well as $\bar{C}_1^3 = \mathbb{1}$, implies also that

$$\tilde{A}_0^2|\psi\rangle = B_0 \otimes \bar{C}_1 |\psi\rangle. \quad (110)$$

We can now use again the first condition in equation (106) but with all local operators being ‘dagged’ (recall that it follows from equation (103) for $n = 2$), which allows us to obtain $\tilde{A}_0^2|\psi\rangle = \tilde{A}_0^\dagger|\psi\rangle$. Since the reduced density matrix corresponding to the first subsystem of $|\psi\rangle$ is full rank, the latter is equivalent to the following relation

$$\tilde{A}_0^2 = \tilde{A}_0^\dagger. \quad (111)$$

Using similar arguments one then shows that \tilde{A}_0 is unitary, which together with (111) implies that $\tilde{A}_0^3 = \mathbb{1}$ and thus \tilde{A}_0 is a proper quantum observable.

Employing then the second and the third relation in equation (106), one can draw the same conclusions for the other two operators on Alice’s side, \tilde{A}_1 and \tilde{A}_2 . As a consequence, all three \tilde{A}_i are quantum observables; in particular, they satisfy

$$\tilde{A}_i^2 = \tilde{A}_i^\dagger \quad (i = 1, 2, 3). \quad (112)$$

Let us now use (112) to characterize A_x observables. By substituting equation (108) into it one finds, after a bit of algebra, that the observables A_x are related via the following formula:

$$\{A_i, A_j\} = -\omega A_k^\dagger, \quad (113)$$

where $i, j, k = 0, 1, 2$ and $i \neq j \neq k$. Using again equation (108) one can also derive similar relations for the tilted observables,

$$\{\tilde{A}_i, \tilde{A}_j\} = -\tilde{A}_k^\dagger \quad (114)$$

with $i, j, k = 0, 1, 2$ such that $i \neq j \neq k$.

Importantly, equation (113) and, analogously, (114) were solved in [24]. In fact, it was proven there (cf fact 5 and corollary 4 in appendix B) that one can identify a qutrit Hilbert space in \mathcal{H}_1 in the sense that $\mathcal{H}_1 = \mathbb{C}^3 \otimes \mathcal{H}'_1$ for some auxiliary Hilbert space \mathcal{H}'_1 , and that there exists a unitary operation $U_1 : \mathcal{H}_1 \rightarrow \mathcal{H}_1$ such that (notice that the third observable \tilde{A}_2 is obtained from the first two by using (114))

$$U_1 \tilde{A}_i U_1 = XZ^i \otimes P_1^{(1)} + (XZ^i)^T \otimes P_2^{(1)} \quad (i = 0, 1, 2), \quad (115)$$

where $P_i^{(1)}$ ($i = 1, 2$) are two projectors such that $P_1^{(1)} + P_2^{(1)} = \mathbb{1}'_1$, where $\mathbb{1}'_1$ is the identity on \mathcal{H}'_1 . There are thus two inequivalent sets of observables at the first site that give rise to the maximal quantum value of our Bell expressions: XZ^i with $i = 0, 1, 2$ and their transpositions.

Step 2. (B_y observables). We can now move on to characterizing the B_y observables. First, by combining the identities in (106) with equation (114) and then by using the fact that \bar{C}_1 and \bar{C}_2 commute as well as that \tilde{A}_i are unitary, one finds the following equations

$$\{B_i, B_j\}|\psi\rangle = -B_k^\dagger|\psi\rangle \quad (116)$$

for all triples i, j, k such that $i \neq j \neq k$. By virtue of the fact that all the single-party reduced density matrices of $|\psi\rangle$ are full rank, these are equivalent to the following matrix equations

$$\begin{aligned}\{B_0, B_1\} &= -B_2^\dagger, \\ \{B_0, B_2\} &= -B_1^\dagger, \\ \{B_1, B_2\} &= -B_0^\dagger,\end{aligned}\tag{117}$$

and thus the B_i observables satisfy analogous relations to A_x . This implies that $\mathcal{H}_2 = \mathbb{C}^3 \otimes \mathcal{H}'_2$ for some auxiliary Hilbert space \mathcal{H}'_2 , and there exists a unitary operation $U_2 : \mathcal{H}_2 \rightarrow \mathcal{H}_2$ such that (cf fact 5 and corollary 4)

$$U_2 B_i U_2^\dagger = ZX^i \otimes P_1^{(2)} + (ZX^i)^T \otimes P_2^{(2)}.\tag{118}$$

for $i = 0, 1, 2$, where $P_1^{(2)}$ and $P_2^{(2)}$ are two orthogonal projectors such that $P_1^{(2)} + P_2^{(2)} = \mathbb{1}'_2$, where $\mathbb{1}'_2$ is the identity acting on \mathcal{H}'_2 (notice that as before the form of the third observable B_2 follows from (117)).

Step 3. ($C_z^{(i)}$ observables). Let us now move on to the $C_z^{(i)}$ observables that are measured by the observers numbered by $i = 3, \dots, N_1 + 1$, and consider the first equation in (106) and the conditions that follow from (104), which for our purposes we state as

$$\tilde{A}_0 \otimes B_0 \otimes [C_0^{(k)}]^{r_{1,k}} \otimes \bar{C}_{0,k} |\psi\rangle = |\psi\rangle\tag{119}$$

and

$$\tilde{A}_{r_{1,k}} \otimes B_0^{r_{1,k}+r_{2,k}} \otimes C_1^{(k)} \otimes \bar{C}'_{0,k} \otimes \bar{D}_k |\psi\rangle = |\psi\rangle\tag{120}$$

with $k = 3, \dots, N_1 + 1$, and

$$\bar{C}_{0,k} = \bigotimes_{\substack{m=3 \\ m \neq k}}^{N_1} [C_0^{(m)}]^{r_{1,m}}, \quad \bar{C}'_{0,k} = \bigotimes_{\substack{m=3 \\ m \neq k}}^{N_1} [C_0^{(m)}]^{r_{1,m}+r_{2,m}}, \quad \bar{D}_k = \bigotimes_{m=N_1+1}^N [D_0^{(m)}]^{r_{k,m}}.\tag{121}$$

Importantly, $r_{1,k} \neq 0$ for any $k = 3, \dots, N_1 + 1$, and hence all equations in (120) contain either \tilde{A}_1 or \tilde{A}_2 . Let us then exploit the fact that all local operators in both equations (119) and (120) are unitary and therefore these equations can be rewritten as

$$\begin{aligned}[C_0^{(k)}]^{r_{1,k}} |\psi\rangle &= \tilde{A}_0^\dagger \otimes B_0^\dagger \otimes \bar{C}_{0,k}^\dagger |\psi\rangle, \\ C_1^{(k)} |\psi\rangle &= \tilde{A}_1^\dagger \otimes B_0^{-(r_{1,k}+r_{2,k})} \otimes [\bar{C}'_{0,k}]^\dagger \otimes \bar{D}_k^\dagger |\psi\rangle.\end{aligned}\tag{122}$$

Crucially, $\bar{C}_{0,k}, \bar{C}'_{0,k}$ commute and therefore we deduce that

$$\left\{ [C_0^{(k)}]^{r_{1,k}}, C_1^{(k)} \right\} |\psi\rangle = \{ \tilde{A}_0, \tilde{A}_1 \}^\dagger \otimes B_0^{\lambda_k} \otimes \bar{C}_{0,k}^\dagger [\bar{C}'_{0,k}]^\dagger \otimes \bar{D}_k^\dagger |\psi\rangle,\tag{123}$$

where for simplicity we denoted $\lambda_k = -(1 + r_{1,k} + r_{2,k})$. In a fully analogous way we can derive

$$\left\{ [C_0^{(k)}]^{r_{1,k}}, C_1^{(k)} \right\}^\dagger |\psi\rangle = \{ \tilde{A}_0, \tilde{A}_1 \} \otimes B_0^{-\lambda_k} \otimes \bar{C}_{0,k} \bar{C}'_{0,k} \otimes \bar{D}_k |\psi\rangle.\tag{124}$$

Both these conditions when combined with equation (114) allow us to conclude that

$$\left\{ [C_0^{(k)}]^{r_{1,k}}, C_1^{(k)} \right\}^\dagger \left\{ [C_0^{(k)}]^{r_{1,k}}, C_1^{(k)} \right\} = \left\{ [C_0^{(k)}]^{r_{1,k}}, C_1^{(k)} \right\} \left\{ [C_0^{(k)}]^{r_{1,k}}, C_1^{(k)} \right\}^\dagger = \mathbb{1}_k,\tag{125}$$

i.e. the above anticommutator is unitary. We can therefore use fact 5 and corollary 4 (see appendix B) which say that for any $k = 3, \dots, N_1 + 1$, $\mathcal{H}_k = \mathbb{C}^3 \otimes \mathcal{H}'_k$ with \mathcal{H}'_k being some auxiliary Hilbert space of unknown dimension, as well as that there exist unitary operations U_k such that

$$U_k [C_0^{(k)}]^{r_{1,k}} U_k^\dagger = Z^{r_{1,k}} \otimes \mathbb{1}'_k,\tag{126}$$

and

$$U_k C_1^{(k)} U_k^\dagger = Z^{r_{1,k}} X \otimes P_1^{(k)} + (Z^{r_{1,k}} X)^T \otimes P_2^{(k)}, \quad (127)$$

where $P_1^{(k)} + P_2^{(k)} = \mathbb{1}'_k$.

Step 4. ($D_w^{(i)}$ observables). Let us finally focus on the D observables. We first consider all vertices $i \in \{N_2 + 2, \dots, N\}$ that are connected to the second vertex. For them $r_{2,k} \neq 0$ and therefore we have from equation (105),

$$B_0^{r_{2,k}} \otimes \tilde{C}_{0,k} \otimes \bar{D}'_{0,k} \otimes D_1^{(k)} |\psi\rangle = |\psi\rangle, \quad (128)$$

where

$$\tilde{C}_{0,k} = \bigotimes_{m=3}^{N_1} [C_0^{(m)}]^{r_{k,m}}, \quad \bar{D}'_{0,k} = \bigotimes_{\substack{i=N_1+1 \\ i \neq k}}^N [D_0^{(i)}]^{r_{k,i}}. \quad (129)$$

At the same time, equation (103) for $k = 1$ gives

$$\tilde{A}_{r_{1,2}} \otimes B_1 \otimes \bar{C}_1 \bar{C}_2 \otimes [D_0^{(k)}]^{r_{2,k}} \otimes \bar{D}_{0,k} |\psi\rangle = |\psi\rangle \quad (130)$$

where

$$\bar{D}_{0,k} = \bigotimes_{\substack{i=N_1+1 \\ i \neq k}}^N [D_0^{(i)}]^{r_{2,i}}. \quad (131)$$

We then rewrite both equations (128) and (131) as

$$\begin{aligned} D_1^{(k)} |\psi\rangle &= B_0^{-r_{2,k}} \otimes \tilde{C}_{0,k}^\dagger \otimes [\bar{D}'_{0,k}]^\dagger |\psi\rangle, \\ [D_0^{(k)}]^{r_{2,k}} |\psi\rangle &= \tilde{A}_1^\dagger \otimes B_1^\dagger \otimes \bar{C}_1^\dagger \bar{C}_2^\dagger \otimes \bar{D}_{0,k}^\dagger |\psi\rangle. \end{aligned} \quad (132)$$

Since as already proven, the anticommutator of $B_0^{-r_{2,k}}$ and B_1 is unitary for any k such that $r_{2,k} \neq 0$, the above equations imply that for all $k = N_1 + 2, \dots, N$ for which $r_{2,k} \neq 0$, the anticommutator of $D_1^{(k)}$ and $[D_0^{(k)}]^{r_{2,k}}$ is unitary too.

We can now move on to those vertices $i \in \{N_1 + 2, \dots, N\}$ that are connected to the remaining neighbours of the first vertex. In this case we proceed in the same way as above, however, we now combine the conditions (104) and (105) as well as we employ the forms of $C_z^{(i)}$ operators given in equations (126) and (127) to observe that for any site k which is connected to a neighbour m of the first vertex the anticommutator of $D_1^{(k)}$ and $[D_0^{(k)}]^{r_{m,k}}$ is unitary and therefore $D_{0/1}^{(k)}$ satisfy the assumptions of fact 5 in appendix B.

Let us finally consider the remaining vertices that are not neighbours of the first vertex. For each of them we can prove that the anticommutator of the local observables $D_{0/1}^{(k)}$ or powers thereof is unitary in a recursive way starting from vertices connected to those that are connected to the neighbours of the first vertex and employing the relations (105). Step by step we can prove the same statement for all D sites exploiting the fact that the graph is connected and therefore for each vertex there is a path connecting it with any other vertex in the graph.

We thus conclude that for all vertices $k = N_1 + 2, \dots, N$ the local Hilbert is $\mathcal{H}_k = \mathbb{C}^3 \otimes \mathcal{H}'_k$ for some finite-dimensional \mathcal{H}'_k and that there exists a unitary U_k such that (cf fact 5 and corollary 4 in appendix B)

$$U_k D_0^{(k)} U_k^\dagger = Z \otimes \mathbb{1}'_k \quad (133)$$

and

$$U_k D_1^{(k)} U_k^\dagger = X \otimes P_1^{(k)} + X^T \otimes P_2^{(k)}. \quad (134)$$

The state. Having determined the form of all local observables we can now move on to proving the self-testing statement for the state. After substituting the above observables, the ‘rotated’ Bell operator corresponding to the Bell inequality which is maximally violated can be expressed as

$$UB_{\mathcal{G}}U^\dagger = \sum_{m_1, \dots, m_N=0}^1 B_{\mathbf{m}} \otimes P_{m_1}^{(1)} \otimes \dots \otimes P_{m_N}^{(N)}, \quad (135)$$

where $U = U_1 \otimes \dots \otimes U_N$ and $P_{m_i}^{(i)}$ are projections introduced above that satisfy $P_1^{(i)}P_2^{(i)} = 0$ for any site $i = 1, \dots, N$, $B_{\mathbf{m}}$ with $\mathbf{m} := m_1 \dots m_N$, where $m_i = 0, 1$, are N -qutrit Bell operators obtained from

$$B = \mathcal{G}_{1,0} + \sum_{l=1}^2 c_{1,l} \mathcal{G}_{1,l} + \sum_{l=3}^{N_1+1} c_{2,l} \mathcal{G}_{2,l} + \sum_{l=N_1+2}^N \mathcal{G}_{3,l} + \text{h.c.}, \quad (136)$$

through the application of the identity map ($m_i = 0$) or the transposition map ($m_i = 1$) to the observables appearing at site i . Here, $\mathcal{G}_{a,b}$ are the stabilising operators of the graph state $|G\rangle$ defined in equations (68) for $n = 1$ and $d = 3$, which for completeness we restate here as

$$\mathcal{G}_{1,0} = X_1 \otimes Z_2 \otimes \bigotimes_{i=3}^{N_1+1} Z_i^{r_{1,i}}, \quad (137)$$

$$\mathcal{G}_{1,k} = (XZ^k)_1 \otimes (ZX^k)_2 \otimes \bigotimes_{i=3}^{N_1+1} Z_i^{r_{1,i}+kr_{2,i}} \otimes \bigotimes_{i=N_1+2}^N Z_i^{kr_{2,i}}, \quad (138)$$

with $k = 1, 2$,

$$\mathcal{G}_{2,k} = (XZ^{r_{1,k}})_1 \otimes Z_2^{r_{1,k}+r_{2,k}} \otimes \bigotimes_{i=3}^{k-1} Z_i^{r_{1,i}+r_{k,i}} \otimes (Z^{r_{1,k}}X)_k \otimes \bigotimes_{i=k+1}^{N_1+1} Z_i^{r_{1,i}+r_{k,i}} \otimes \bigotimes_{i=N_2+2}^N Z_i^{r_{k,i}} \quad (139)$$

with $k = 3, \dots, N_1 + 1$

$$\mathcal{G}_{3,k} = Z_2^{r_{2,k}} \otimes \bigotimes_{i=3}^{N_1+1} Z_i^{r_{k,i}} \otimes \bigotimes_{i=N_1+2}^{k-1} Z_i^{r_{k,i}} \otimes X_k \otimes \bigotimes_{i=k+1}^N Z_i^{r_{k,i}}, \quad (140)$$

with $k = N_1 + 2, \dots, N$. The subscripts were added to X and Z to denote the site at which these operators act; recall also that we fixed $r_{1,2} = 1$.

The formula (135) takes into account the fact that at each site we have two choices of measurements, with and without the transposition. Thus, the Bell operator is composed of 2^N N -qutrit Bell operators. For instance, for $m_1 = \dots = m_N = 0$ no partial transposition is applied to B and therefore $B_{0\dots 0} \equiv B$, whereas for $m_1 = \dots = m_N = 1$ the partial transposition is applied to every site and hence $B_{1\dots 1} = B^T$, where T stands for the global transposition.

In order to find the form of the state maximally violating our inequality we now determine the eigenvector(s) of the Bell operator $B_{\mathcal{G}}$ corresponding its maximal eigenvalue which is $2(N - N_1 + d - 1)$ (cf equation (86)). To this end, let us focus on the N -qutrit operators $B_{\mathbf{m}}$ and prove that the latter number is an eigenvalue of only two of them, B and B^T , which correspond to the cases $m_1 = m_2 = \dots = m_N = 0, 1$, whereas the eigenvalues of the remaining operators are all lower.

Clearly, B is composed of the stabilising operators of the graph state $|G\rangle$ and therefore its maximal eigenvalue coincides with the maximal quantum violation of the inequality which is $2(N - N_1 + d - 1)$. The same applies to B^T because the transposition does not change the eigenvalues and the graph state is real.

Let us then move on to the remaining cases, i.e. m_i are not all equal. We will show that in all those $2^N - 2$ cases the $B_{\mathbf{m}}$ operators have eigenvalues lower than $2(N - N_1 + 2)$ because for all those cases one can pick a few stabilizing operators $\mathcal{G}_{a,b}$ whose partial transpositions cannot stabilize a common pure state anymore. For further benefits let us denote by $\mathcal{G}_{a,b}^{\mathbf{m}}$ the stabilizing operators which are partially transposed with respect to those subsystems i for which $m_i = 1$. We divide the proof into three parts corresponding to three cases: (i) $m_1 = m_2 = 0$, (ii) $m_1 = m_2 = 1$ and (iii) $m_1 = 0, m_2 = 1$ or $m_1 = 1, m_2 = 0$, and also a few sub-cases.

- The first one assumes that either $m_1 = 1$ and $m_2 = 0$ or $m_1 = 0$ and $m_2 = 1$, i.e. we take the transposed observables at the first or the second site, but not both at the same time. For simplicity let us then fix $m_1 = 1$ and $m_2 = 0$. We consider three operators $\mathcal{G}_{1,i}^{T_1}$ with $i = 0, 1, 2$, where T_1 is the transposition applied to

the observables at the first site. It is not difficult to observe that using the explicit forms of the stabilizing operators (cf equations (137) and (138)) and including the transposition at the first site, one obtains

$$\mathcal{G}_{1,0}^{T_1} \mathcal{G}_{1,1}^{T_1} \mathcal{G}_{1,2}^{T_1} = [X^T(XZ)^T(XZ^2)^T]_1 \otimes [ZZXZX^2]_2, \quad (141)$$

where we also used the fact that the products of the observables at the remaining sites amounts to identity. Using then the fact that $ZX = \omega XZ$, the above simplifies to

$$\mathcal{G}_{1,0}^{T_1} \mathcal{G}_{1,1}^{T_1} \mathcal{G}_{1,2}^{T_1} = \omega \mathbb{1}. \quad (142)$$

This simple fact precludes that there exists a common eigenvector of $\mathcal{G}_{1,i}^{T_1}$ ($i = 1, 2, 3$) with eigenvalue one.

- Next, we consider the case when the observables at the first two sites are not transposed, i.e. $m_1 = m_2 = 0$. There thus exists $i \neq 1, 2$ such that $m_i = 1$. Let us first assume that this particular vertex belongs to $i \in \{3, \dots, N_1 + 1\}$, i.e. we take the transposed observables for this site. We then consider two operators $\mathcal{G}_{1,0}$ and $\mathcal{G}_{2,i}$. Notice then that the first of these operators has the Z observable at site i because $i \in \mathcal{N}_1$, i.e. it is connected to the first vertex, whereas the second one has $Z^{r_{1,i}}X$ at this position. At the remaining positions different than the first two they have only Z observable or the identity which do not feel the action of transposition. All this means that in this case $\mathcal{G}_{1,0}^m = \mathcal{G}_{1,0}$ and $\mathcal{G}_{2,i}^m = \mathcal{G}_{2,i}^{T_i}$. Due to the fact that the transposition at site i modifies X appearing in $\mathcal{G}_{2,i}$ to X^\dagger , the operators $\mathcal{G}_{1,0}$ and $\mathcal{G}_{2,i}^{T_i}$ do not commute (recall that by the very definition the stabilising operators without the transposition commute). By virtue of fact 4 stated in appendix A this implies that $\mathcal{G}_{1,0}$ and $\mathcal{G}_{2,i}^{T_i}$ do not stabilize a common pure state.

Let us now move on to the second sub-case in which $m_i = 1$ for any $i \in \mathcal{N}_1$ and there exist $i \in \{N_1 + 2, \dots, N\}$ such that $m_i = 2$. Since the graph is connected there exist another vertex $j \neq 1, i$ which is connected to i . Analogously to the previous case, we consider two operators: $\mathcal{G}_{3,i}^m$ and one of $\mathcal{G}_{a,b}^m$, where the choice of the latter operator is dictated by the choice of the vertex j which i is connected to: for $j = 2$ we take $\mathcal{G}_{1,1}^m$; for $j \in \{3, \dots, N_1 + 1\}$ we take $\mathcal{G}_{2,j}^m$; finally, for $j \in \{N_1 + 2, \dots, N\}$ we take $\mathcal{G}_{3,j}^m$.

Now, $\mathcal{G}_{3,i}^m$ has the X operator at site i and the Z operator at the remaining ‘ D ’ sites, whereas all the other operators $\mathcal{G}_{a,b}^m$ for $a = 1, 2, 3$ and $b \neq i$ listed above have only either the Z operator or the identity at all ‘ D ’ sites. Thus, $\mathcal{G}_{a,b}^m = \mathcal{G}_{a,b}$ for any $a = 1, 2, 3$ and $b \neq i$ and any sequence \mathbf{m} in which $m_l = 1$ for $l = 1, \dots, N_1 + 1$, and $\mathcal{G}_{3,i}^m = \mathcal{G}_{3,i}^{T_i}$. Now, it clearly follows that $\mathcal{G}_{3,i}^m$ does not commute with the chosen $\mathcal{G}_{a,b}$ because the transposition at site i changes the X operator to X^2 and because, by the very definition, $\mathcal{G}_{3,i}$ (without the transposition) commutes with any other $\mathcal{G}_{a,b}$. As before this implies that $\mathcal{G}_{3,i}^m \mathcal{G}_{a,b} = \omega^q \mathcal{G}_{a,b} \mathcal{G}_{3,i}^m$ for some $q = 1, 2$, and therefore these two operators cannot stabilize a common pure state (cf fact 4 in appendix A).

- The last case to consider is when $m_1 = m_2 = 1$; the remaining m_i can take arbitrary values except for being all equal to one, which corresponds to the already-considered case of all observables being transposed. Here we can use the fact that $\mathcal{G}_{a,b}^m$ for all a, b stabilize the graph state $|\psi\rangle$ if and only if $[\mathcal{G}_{a,b}^m]^T$ does, where T is the global transposition. We can thus apply the global transposition to all the operators $\mathcal{G}_{a,b}^m$ and consider again the case when $m_0 = m_2 = 0$ and there is some $i \neq 1, 2$ such that $m_i = 1$, which has already been considered above.

Knowing that among all the $B_{\mathbf{m}}$ operators only B and B^T give rise to the maximal quantum violation of the Bell inequality corresponding to the considered graph, we can determine the form of the state $|\psi\rangle$ maximally violating the inequality. Due to the fact that each local Hilbert space decomposes as $\mathcal{H}_k = \mathbb{C}^3 \otimes \mathcal{H}'_k$ we can write the state as

$$|\psi\rangle = \sum_{i_1, \dots, i_N} |\psi_{i_1, \dots, i_N}\rangle \otimes |i_1\rangle_1 \otimes \dots \otimes |i_N\rangle_N, \quad (143)$$

where $|\psi'\rangle = (U_1 \otimes \dots \otimes U_N)|\psi\rangle$, $|\psi_{i_1, \dots, i_N}\rangle$ are some vectors from $(\mathbb{C}^3)^{\otimes N}$ and the local bases $|i_k\rangle$ are the eigenbases of the projectors $P_{m_k}^{(k)}$. The fact that $|\psi\rangle$ achieves the maximal quantum value of the inequality, $\beta_Q = 2(N - N_1 + 2)$, means that the following identity

$$\mathcal{B}_G |\psi\rangle = 2(N - N_1 + 2) |\psi\rangle \quad (144)$$

holds true. Plugging equations (143) and (135) into the above equation one finds that it is satisfied iff for every sequence \mathbf{m} ,

$$B_{\mathbf{m}} |\psi_{i_1, \dots, i_N}\rangle = 2(N - N_1 + 2) |\psi_{i_1, \dots, i_N}\rangle, \quad (145)$$

holds true for all those sequences i_1, \dots, i_N for which the local vectors $|i_k\rangle$ at site k are the eigenvectors of the operator $P_{m_k}^{(k)}$. As already discussed above, this condition can be met for only two of these operators, B and B^T .

Moreover, the stabilising operators that B (and thus also B^T) are composed of stabilize a unique state, which is the graph state $|G\rangle$. Consequently, $|\psi_{i_1, \dots, i_N}\rangle = |G\rangle$ for any sequence i_1, \dots, i_N for which the corresponding local vectors are the eigenvectors of $P_0^{(k)}$ (or $P_1^{(k)}$ in the case of B^T).

On the other hand, we showed that the eigenvalues of the remaining operators B_m are lower than the maximal violation of the Bell inequality and thus in all those cases equation (145) can be satisfied iff the corresponding vectors vanish, $|\psi_{i_1, \dots, i_N}\rangle = 0$. Taking all this into account, we conclude that the state $|\psi'\rangle$ has the following form

$$(U_1 \otimes \dots \otimes U_N)|\psi\rangle = |\psi_G\rangle \otimes |\varphi\rangle, \quad (146)$$

where $|\varphi\rangle$ is some state from the auxiliary Hilbert spaces $\mathcal{H}'_1 \otimes \dots \otimes \mathcal{H}'_N$ that satisfies

$$\left(P_i^{(1)} \otimes \dots \otimes P_i^{(N)}\right) |\varphi\rangle = |\varphi\rangle \quad (i = 0, 1). \quad (147)$$

This completes the proof. □

5. Conclusions and outlook

In this work we introduced a family of Bell expressions whose maximal quantum values are achieved by graph states of arbitrary prime local dimension. While at the moment we are unable to compute their maximal classical values, we believe the corresponding Bell inequalities are all nontrivial. This belief is supported by a few examples of Bell expressions for which the classical bound was found numerically, and the fact that in the particular case of qutrit states they enable self-testing of all graph states. We thus introduced a broad class of Bell inequalities that can be used for testing non-locality of many interesting and relevant multipartite states, including the absolutely maximally entangled states. Moreover, in the particular case of many-qutrit systems our inequalities can also be employed to self-test the graph states, in particular the four-qutrit absolutely maximally entangled state.

There is a few possible directions for further research that are inspired by our work:

- First, it would be interesting to generalize our method to the case of composite d , in particular for prime powers. The present approach is based on that of [24] which, in order to prove that the linear combinations in equation (31) are unitary operators which when raised to d are identities employed certain relations for quadratic Gauss sums that hold true for prime d .
- Second of all, as far as implementations of self-testing are concerned it is a problem of a high relevance to understand how robust our self-testing statements are against noises and experimental imperfections.
- Another possible direction that is related to the possibility of experimental implementations of self-testing is to find Bell inequalities maximally violated by graph states that require performing the minimal number of two measurement per observer to self-test the state. For instance, for the GHZ state such a Bell inequality [27] and a self-testing scheme [29] (see also [28]) based on the maximal violation of this inequality were introduced recently; this inequality is based, however, on a slightly different construction which is not directly related to the stabilizer formalism used by us here.
- Fourth, it is interesting to explore whether one can derive self-testing statements based on the maximal violation of our inequalities for higher prime dimensions $d \geq 0$. While it is already known (see [24]) that these inequalities do not serve the purpose as far as quantum observables are concerned because there exist many different choices of them that are not unitarily equivalent (such as those appearing in the proof of theorem 3 for $d = 3$ which are related by the transposition), whether they enable self-testing of graph states remains open. In other words, it is unclear whether the given graph state is the only one (up to the above equivalences) that meets the necessary and sufficient conditions for the maximal quantum violation of the corresponding Bell inequality stemming from the sum-of-squares decomposition.
- The fifth possible direction is to generalize our construction so that it allows for designing Bell inequalities that are maximally violated by other classes of states such as for instance the hyper-graph states [43] (see also [44] in this context).
- Last but not least, one can also explore the possibility of self-testing of genuinely entangled subspaces within the stabiliser formalism in Hilbert spaces of arbitrary prime local dimension along the lines of [22, 23].

Data availability statement

No new data were created or analysed in this study.

Acknowledgments

We acknowledge the VERIQTAS project funded within the QuantERA II Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101017733 and the Polish National Science Centre (Grant No. 2021/03/Y/ST2/00175). F B is supported by the Alexander von Humboldt foundation.

Appendix A. A few facts

Fact 2. Consider the generalized Pauli matrices defined through the following formulas

$$X|i\rangle = |i+1\rangle, \quad Z|i\rangle = \omega^i|i\rangle, \quad (148)$$

where $|i\rangle$ ($i = 0, \dots, d-1$) are the elements of the standard basis of \mathbb{C}^d . There are no complex numbers $\alpha, \beta \neq 0$ for which $\alpha X + \beta Z$ is unitary.

Proof. The proof is elementary. We first expand

$$(\alpha X + \beta Z)^\dagger (\alpha X + \beta Z) = (|\alpha|^2 + |\beta|^2) \mathbb{1} + \alpha^* \beta X^\dagger Z + \beta^* \alpha Z^\dagger X. \quad (149)$$

Let us then show that for any $d \geq 3$, the operators $X^\dagger Z$ and $Z^\dagger X$ are linearly independent. To this end, we assume that $X^\dagger Z$ and $Z^\dagger X$ are linearly dependent and thus $X^\dagger Z = \eta Z^\dagger X$ for some $\eta \in \mathbb{C}$. By using the fact that $ZX = \omega XZ$, we can rewrite this equation as $X^\dagger Z = \eta \omega^{d-1} XZ^\dagger$, which, taken into account the fact that X and Z are unitary further rewrites as $Z^2 = \eta \omega^{d-1} X^2$ which for $d \geq 3$ is satisfied iff $\eta = 0$.

It now follows that the expression (149) equals $\mathbb{1}$ if and only if α or β vanishes. This completes the proof. \square

Let us notice that the above fact fails to be true for $d = 2$ because in this case $ZX = -XZ$ and therefore XZ and ZX are linearly dependent, which makes it possible to find α, β such that $\alpha X + \beta Z$ is unitary. In fact, any pair of real positive numbers obeying $\alpha^2 + \beta^2 = 1$ makes this matrix unitary.

Let us finally provide a proof of the properties (39) and (40). For this purpose we recall $\tilde{A}_k^{(n)}$ to be given by

$$\tilde{A}_k^{(n)} := \frac{\omega^{-nk(k+1)}}{\sqrt{d}\lambda_n} \sum_{t=0}^{d-1} \omega^{-ntk} A_t^n, \quad (150)$$

where A_t are unitary observables.

Fact 3. Consider the following matrices

$$\tilde{A}_k^{(n)} := \frac{\omega^{-nk(k+1)}}{\sqrt{d}\lambda_n} \sum_{t=0}^{d-1} \omega^{-ntk} A_t^n, \quad (151)$$

where A_t are unitary observables. For any $n = 0, \dots, d-1$, the following identity holds true:

$$\sum_{k=0}^{d-1} \tilde{A}_k^{(d-n)} \tilde{A}_k^{(n)} = \sum_{k=0}^{d-1} \left[\tilde{A}_k^{(n)} \right]^\dagger \tilde{A}_k^{(n)} = d\mathbb{1}. \quad (152)$$

Proof. After plugging equation (151) into equation (152), one obtains

$$\sum_{k=0}^{d-1} \tilde{A}_k^{(d-n)} \tilde{A}_k^{(n)} = \frac{1}{d|\lambda_n|^2} \sum_{s,t=0}^{d-1} \sum_{k=0}^{d-1} \omega^{nk(s-t)} A_s^{-n} A_t^n. \quad (153)$$

Employing then the following identity

$$\sum_{k=0}^{d-1} \omega^{nk(s-t)} = d\delta_{s,t} \quad (154)$$

and the fact that $|\lambda_n|^2 = 1$ for any n , one directly arrives at equation (152), which completes the proof. \square

Fact 4. Consider two N-qudit operators S_1 and S_2 which are N-fold tensor products of $X^i Z^j$ with $i, j = 0, \dots, d-1$ with prime d . Assume also that $S_1^d = S_2^d = \mathbb{1}$. If $[S_1, S_2] \neq 0$, then they cannot stabilize a common pure state in; in other words, no nonzero $|\psi\rangle \in (\mathbb{C}^d)^{\otimes N}$ exists such that $S_i |\psi\rangle = |\psi\rangle$ for $i = 1, 2$.

Proof. Let us first notice that the Weyl–Heisenberg matrices $W_{i,j} = X^i Z^j$ satisfy the following commutation relations $W_{i,j} W_{k,l} = \omega^{f(i,j,k,l)} W_{k,l} W_{i,j}$ with $f: \{0, \dots, d-1\}^4 \rightarrow \{0, \dots, d-1\}$, and thus there exists $q = \{1, \dots, d-1\}$ such that

$$S_1 S_2 = \omega^q S_2 S_1 \quad (q = 1, \dots, d-1), \quad (155)$$

where $q \neq 0$ due to the assumption that S_i do not commute.

Now, let us assume that S_i stabilise a common pure state, $S_i |\psi\rangle = |\psi\rangle$ for $i = 1, 2$. Then, the relation (155) implies $|\psi\rangle = \omega^q |\psi\rangle$ which is satisfied iff $|\psi\rangle = 0$, which leads to a contradiction. This ends the proof. \square

Appendix B. Characterisation of observables

The following proposition was proven in appendix B of [24].

Fact 5. Let R_0 and R_1 acting on some finite-dimensional Hilbert space \mathcal{B} be unitary operators satisfying $R_0^3 = R_1^3 = \mathbb{1}$. If the anticommutator $\{R_0, R_1\}$ is unitary, then $\mathcal{H} = \mathbb{C}^3 \otimes \mathcal{H}'$ for some Hilbert space \mathcal{H}' and there exists a unitary $U: \mathcal{H} \rightarrow \mathbb{C}^3 \otimes \mathcal{H}'$ such that

$$\begin{aligned} UR_0 U^\dagger &= X \otimes Q + X \otimes Q^\perp = X \otimes \mathbb{1}', \\ UR_1 U^\dagger &= X^2 Z \otimes Q + Z^2 \otimes Q^\perp, \end{aligned} \quad (156)$$

where Q and Q^\perp are orthogonal projections satisfying $Q + Q^\perp = \mathbb{1}'$ and $\mathbb{1}'$ stands for the identity acting on \mathcal{H}' .

Based on the above fact let us now show demonstrate that for each of the subsets of observables $A_x, B_y, C_z^{(i)}$ and $D_w^{(i)}$ there exist local unitary operations bringing them to the forms used in equations (115), (118), (126) and (127), and finally, (133) and (134).

Corollary 4. The following statements can be verified by a direct check:

- **(A_x observables)** By using $\mathcal{U}_1 = F^\dagger V_1 F \otimes Q_1 + F^\dagger V_1^* V_2 F \otimes Q_2$, where F, V_1 and V_2 are unitary operations given by

$$F = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad V_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{pmatrix}, \quad V_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad (157)$$

one can bring the observables in equation (156) into the following form used in equation (115):

$$\begin{aligned} X \otimes Q + X^T \otimes Q^\perp, \\ XZ \otimes Q + (XZ)^T \otimes Q^\perp. \end{aligned} \quad (158)$$

- **(B_y and $C_z^{(i)}$ observables)** By using $\mathcal{U}_2 = V_3 F \otimes Q + (V_1 V_3)^* F \otimes Q^\perp$, and relabelling $Q \leftrightarrow Q^\perp$ one brings the observables (156) to those in equation (118), that is,

$$\begin{aligned} Z \otimes Q + Z \otimes Q^\perp &= Z \otimes \mathbb{1}, \\ ZX \otimes Q + (ZX)^T \otimes Q^\perp, \end{aligned} \quad (159)$$

where

$$V_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}. \quad (160)$$

Then, by applying $\mathcal{U}_3 = (V_1 V_3)^* \otimes Q + V_2' \otimes Q^\perp$ operation we can bring (159) to

$$\begin{aligned} Z \otimes Q + Z \otimes Q &= Z \otimes \mathbb{1}, \\ Z^2 X \otimes Q + (Z^2 X)^T \otimes Q^\perp. \end{aligned} \quad (161)$$

Depending on the value of $r_{1,k} \neq 0$, both (159) and (161) are used in equations (126) and (127).

- ($D_w^{(i)}$ observables) By applying $\mathcal{U}_4 = V_1 V_3 \otimes Q + (V_1 V_3)^* \otimes Q^\perp$ to the above observables (159) one can bring them to the following form

$$\begin{aligned} Z \otimes Q + Z \otimes Q^\perp &= Z \otimes \mathbb{1}, \\ X \otimes Q + X^T \otimes Q^\perp, \end{aligned} \quad (162)$$

which is used in equations (133) and (134).

ORCID iD

Remigiusz Augusiak  <https://orcid.org/0000-0003-1154-6132>

References

- [1] Bell J S 1964 On the Einstein-Podolsky-Rosen paradox *Phys. Phys. Fiz.* **1** 195
- [2] Brunner N, Pironio S, Acín A, Gisin N, Méthot A A and Scarani V 2008 Testing the dimension of hilbert spaces *Phys. Rev. Lett.* **100** 210503
- [3] Moroder T, Bancal J-D, Liang Y-C, Hofmann M and Gühne O 2013 Device-independent entanglement quantification and related applications *Phys. Rev. Lett.* **111** 030501
- [4] Pironio S *et al* 2010 Random numbers certified by Bell's theorem *Nature* **464** 1021–4
- [5] Acín A, Massar S and Pironio S 2012 Randomness versus nonlocality and entanglement *Phys. Rev. Lett.* **108** 100402
- [6] Acín A, Pironio S, Vértesi T and Wittek P 2016 Optimal randomness certification from one entangled bit *Phys. Rev. A* **93** 040102
- [7] Woodhead E, Kaniewski J, Bourdoncle B, Salavrakos A, Bowles J, Acín A and Augusiak R 2020 Maximal randomness from partially entangled states *Phys. Rev. Res.* **2** 042028
- [8] Mayers D and Yao A 2004 Self testing quantum apparatus *Quantum Inf. Comput.* **4** 273
- [9] Wu D *et al* 2021 Robust self-testing of multipartite entanglement *Phys. Rev. Lett.* **127** 230503
- [10] Yang B, Raymond R, Imai H, Chang H and Hiraishi H 2022 Testing scalable Bell inequalities for quantum graph states on ibm quantum devices *IEEE J. Emerg. Sel. Top. Circuits Syst.* **12** 638–47
- [11] Šupić I and Bowles J 2020 Self-testing of quantum systems: a review *Quantum* **4** 337
- [12] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880–4
- [13] Collins D, Gisin N, Linden N, Massar S and Popescu S 2002 Bell inequalities for arbitrarily high-dimensional systems *Phys. Rev. Lett.* **88** 040404
- [14] Barrett J, Kent A and Pironio S 2006 Maximally nonlocal and monogamous quantum correlations *Phys. Rev. Lett.* **97** 170409
- [15] Laskowski W, Paterek T, Żukowski M and Brukner Č 2004 Tight multipartite Bell's inequalities involving many measurement settings *Phys. Rev. Lett.* **93** 200401
- [16] Żukowski M and Brukner Č 2002 Bell's theorem for general n-qubit states *Phys. Rev. Lett.* **88** 210401
- [17] Gühne O, Tóth G, Hyllus P and Briegel H J 2005 Bell inequalities for graph states *Phys. Rev. Lett.* **95** 120405
- [18] Tóth G, Gühne O and Briegel H J 2006 Two-setting Bell inequalities for graph states *Phys. Rev. A* **73** 022303
- [19] Salavrakos A, Augusiak R, Tura J, Wittek P, Acín A and Pironio S 2017 Bell inequalities tailored to maximally entangled states *Phys. Rev. Lett.* **119** 040402
- [20] Baccari F, Augusiak R, Šupić I, Tura J and Acín A 2020 Scalable Bell inequalities for qubit graph states and robust self-testing *Phys. Rev. Lett.* **124** 020402
- [21] McKague M 2011 Self-testing graph states *Conf. Quantum Computation, Communication and Cryptography (Lecture Notes in Computer Science vol 6745)* (Springer) pp 104–20 (available at: https://link.springer.com/chapter/10.1007/978-3-642-54429-3_7)
- [22] Baccari F, Augusiak R, Šupić I and Acín A 2020 Device-independent certification of genuinely entangled subspaces *Phys. Rev. Lett.* **125** 260507
- [23] Makuta O and Augusiak R 2021 Self-testing maximally-dimensional genuinely entangled subspaces within the stabilizer formalism *New J. Phys.* **23** 043042
- [24] Kaniewski J, I Šupić, Tura J, Baccari F, Salavrakos A and Augusiak R 2019 Maximal nonlocality from maximal entanglement and mutually unbiased bases and self-testing of two-qutrit quantum systems *Quantum* **3** 198
- [25] Tavakoli A, Farkas M, Rosset D, Bancal J-D and Kaniewski J 2021 Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments *Sci. Adv.* **7** eabc3847
- [26] Pereira Alves G and Kaniewski J 2022 Optimality of any pair of incompatible rank-one projective measurements for some nontrivial Bell inequality *Phys. Rev. A* **106** 032219
- [27] Augusiak R, Salavrakos A, Tura J and Acín A 2019 Bell inequalities tailored to the Greenberger-Horne-Zeilinger states of arbitrary local dimension *New J. Phys.* **21** 113001
- [28] Sarkar S, Saha D, Kaniewski J and Augusiak R 2019 Self-testing quantum systems of arbitrary local dimension with minimal number of measurements *npj Quantum Inf.* **7** 151
- [29] Sarkar S and Augusiak R 2022 Self-testing of multipartite Greenberger-Horne-Zeilinger states of arbitrary local dimension with arbitrary number of measurements per party *Phys. Rev. A* **105** 032416
- [30] Briegel H J and Raussendorf R 2001 Persistent entanglement in arrays of interacting particles *Phys. Rev. Lett.* **86** 910–3
- [31] Helwig W 2013 Absolutely maximally entangled qudit graph states (arXiv:1306.2879)
- [32] Yao X-C *et al* 2012 Experimental demonstration of topological error correction *Nature* **482** 489–94
- [33] Raussendorf R and Briegel H J 2001 A one-way quantum computer *Phys. Rev. Lett.* **86** 5188–91
- [34] Briegel H J, Browne D E, Dür W, Raussendorf R and den Nest M V 2009 Measurement-based quantum computation *Nat. Phys.* **5** 19–26
- [35] Tóth G and Apellaniz I 2014 Quantum metrology from a quantum information science perspective *J. Phys. A: Math. Theor.* **47** 424006
- [36] Slofstra W 2019 The set of quantum correlations is not closed *Forum of Math. Pi.* **7**

- [37] Kaniewski J 2020 Weak form of self-testing *Phys. Rev. Res.* **2** 033420
- [38] Schlingemann D and Werner R F 2001 Quantum error-correcting codes associated with graphs *Phys. Rev. A* **65** 012308
- [39] Hostens E, Dehaene J and De Moor B 2005 Stabilizer states and clifford operations for systems of arbitrary dimensions and modular arithmetic *Phys. Rev. A* **71** 042315
- [40] Hein M, Dür W, Eisert J, Raussendorf R, Nest M and Briegel H-J 2006 Entanglement in graph states and its applications (arXiv:quant-ph/0602096)
- [41] Facchi P, Florio G, Parisi G and Pascazio S 2008 Maximally multipartite entangled states *Phys. Rev. A* **77** 060304
- [42] Cervera-Lierta A, Latorre J I and Goyeneche D 2019 Quantum circuits for maximally entangled states *Phys. Rev. A* **100** 022342
- [43] Rossi M, Huber M, Bruß D and Macchiavello C 2013 Quantum hypergraph states *New J. Phys.* **15** 113022
- [44] Gachechiladze M, Budroni C and Gühne O 2016 Extreme violation of local realism in quantum hypergraph states *Phys. Rev. Lett.* **116** 070401

Chapter 5

Concluding remarks

In this thesis, we proposed schemes for certification of quantum systems based on maximal violation of noncontextuality inequalities and Bell inequalities targeted to special quantum realizations. It is known from some recent works that Bell inequalities and noncontextuality inequalities are useful for such a purpose [18]. In this thesis, we generalized some results known from the literature [75]-[22]-[88]-[89]-[68]-[10] and we were able to drop some strong assumptions made about the quantum devices used in the protocol of certification. One of the main challenges targeted in this thesis was to find noncontextuality or Bell inequalities that are maximally violated by certain states and measurements. Another challenge was to design contextuality-based certification schemes that rely on less assumptions about the considered physical systems as compared to the existing results [25], [77] and thus make them as device-independent as possible.

In order to find the desired inequalities, we extensively exploited the stabilizer formalism which often allows to construct the related the sum-of-squares (SOS) decompositions. We believe that suitable adaptations of our approach may lead to noncontextuality or Bell inequalities tailored to other states and measurements beyond those considered in this thesis. Also, beyond the analytical approaches presented in this thesis, the numerical techniques such as those based on the semi-definite programming [21], [77], can be very helpful in achieving this aim.

Let us also comment here about the scalability of our methods with the system size. While an increasing number of measurements and expectation values that the certification schemes are based on can facilitate the mathematical solutions, they might be a problem as far as experimental implementations are concerned. Moreover, it is a highly non-trivial question to explore what is the minimal amount of information about the observed nonclassical correlations that enable making non-trivial statements about the underlying quantum system.

Another direction for further study, as far as implementations of our certification schemes are concerned is to explore whether they are robust to noises and experimental imperfections. When dealing with experimental errors, we have to be aware on how sensitive our methods are to small deviations close to the optimal quantum violation. However, such a robustness analysis is in general a highly nontrivial problem as far as analytical methods are concerned, and therefore in this thesis we present such an analysis only in a particular case. A possible alternative to handle such problems would be to implement numerical methods.

From a more general perspective, it would be interesting to design a unifying approach to self-testing based on Bell nonlocality and contextuality. Despite nonlocality being a specific instance of

contextuality, practical challenges emerge when formulating certification schemes based on these forms of non-classicality. For instance, in the case of spatially separated systems, commutativity between measurements performed in different locations is a natural consequence, while for systems for which spatial separation cannot be guaranteed, compatibility of measurements can be an issue to be tackled and this was one of the challenges we addressed in this thesis.

Bibliography

- [1] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?” *Phys. Rev.*, vol. 47, 777–780, 10 1935. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRev.47.777>.
- [2] J. S. Bell, “On the Einstein-Podolsky-Rosen paradox,” *Physics Physique Fizika*, vol. 1, 195–200, 3 1964. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195>.
- [3] S. J. Freedman and J. F. Clauser, “Experimental test of local hidden-variable theories,” *Phys. Rev. Lett.*, vol. 28, 938–941, 14 1972. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.28.938>.
- [4] A. Aspect, J. Dalibard, and G. Roger, “Experimental test of Bell’s inequalities using time-varying analyzers,” *Phys. Rev. Lett.*, vol. 49, 1804–1807, 25 1982. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.49.1804>.
- [5] B. Hensen and et al., “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres,” *Nature*, vol. 526, 682–686, 5 2015. [Online]. Available: <https://www.nature.com/articles/nature15759#citeas>.
- [6] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, “Bell nonlocality,” *Reviews of Modern Physics*, vol. 86, no. 2, 419–478, 2014. [Online]. Available: <https://doi.org/10.1103/2Frevmodphys.86.419>.
- [7] E. P. Specker and S. Kochen, “The problem of hidden variables in quantum mechanics,” *Indiana Univ. Math. J.*, vol. 17, 59–87, 1 1968.
- [8] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Bell’s theorem, quantum theory, and conceptions of the universe,” in, ser. Fundamental Theories of Physics, vol. 37, Springer Dordrecht, 1989, 69–72.
- [9] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” *Phys. Rev. Lett.*, vol. 23, 880–884, 15 1969. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.23.880>.
- [10] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky, “Simple test for hidden variables in spin-1 systems,” *Phys. Rev. Lett.*, vol. 101, 020403, 2 2008. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.101.020403>.
- [11] R. Cleve and H. Buhrman, “Substituting quantum entanglement for communication,” *Phys. Rev. A*, vol. 56, 1201–1204, 2 1997. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.56.1201>.

- [12] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, “Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem,” 2001. [Online]. Available: <https://arxiv.org/abs/quant-ph/0106052>.
- [13] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, “Zero-error channel capacity and simulation assisted by non-local correlations,” *IEEE Transactions on Information Theory*, vol. 57, no. 8, 5509–5523, 2011. [Online]. Available: <https://doi.org/10.1109/2Ftit.2011.2159047>.
- [14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, “Device-independent security of quantum cryptography against collective attacks,” *Phys. Rev. Lett.*, vol. 98, 230501, 23 2007. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.98.230501>.
- [15] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, 661–663, 6 1991. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.67.661>.
- [16] A. Touzalín, C. Marcus, F. Heijman, E. Cirac, R. Murray, and T. Calarco, “Quantum manifesto,” 2016. [Online]. Available: <http://qurope.eu/manifesto>.
- [17] D. Mayers and A. Yao, “Self testing quantum apparatus,” 2003. [Online]. Available: <https://arxiv.org/abs/quant-ph/0307205>.
- [18] I. Šupić and J. Bowles, “Self-testing of quantum systems: A review,” *Quantum*, vol. 4, 337, Sep. 2020. [Online]. Available: <https://doi.org/10.22331/q-2020-09-30-337>.
- [19] T. H. Yang and M. Navascués, “Robust self-testing of unknown quantum systems into any entangled two-qubit states,” *Phys. Rev. A*, vol. 87, 050102, 5 2013. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.87.050102>.
- [20] A. Coladangelo, K. T. Goh, and V. Scarani, “All pure bipartite entangled states can be self-tested,” *Nature Communications*, vol. 8, no. 1, 2017. [Online]. Available: <https://doi.org/10.1038/2Fncomms15485>.
- [21] C. Bamps and S. Pironio, “Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing,” *Phys. Rev. A*, vol. 91, 052111, 5 2015. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.91.052111>.
- [22] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín, “Scalable Bell inequalities for qubit graph states and robust self-testing,” *Phys. Rev. Lett.*, vol. 124, 020402, 2 2020. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.124.020402>.
- [23] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, “Self-testing protocols based on the chained Bell inequalities,” *New Journal of Physics*, vol. 18, no. 3, 035013, 2016. [Online]. Available: <https://doi.org/10.1088/2F1367-2630/2F18%2F3%2F035013>.
- [24] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, “Self-testing quantum systems of arbitrary local dimension with minimal number of measurements,” *npj Quantum Information*, vol. 7, no. 1, 2021. [Online]. Available: <https://doi.org/10.1038/2Fs41534-021-00490-3>.
- [25] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L.-C. Kwek, “Robust self-testing of quantum systems via noncontextuality inequalities,” *Phys. Rev. Lett.*, vol. 122, 250403, 25 2019. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.122.250403>.

- [26] B. Amaral and M. T. Cunha, *On graph approaches to contextuality and their role in quantum theory*, ser. SpringerBriefs in Mathematics. Springer, 2018. [Online]. Available: <https://link.springer.com/book/10.1007/978-3-319-93827-1>.
- [27] Y.-C. Liang, R. W. Spekkens, and H. M. Wiseman, “Specker’s parable of the overprotective seer: A road to contextuality, nonlocality and complementarity,” *Physics Reports*, vol. 506, 1–39, 2011, Cleaning large correlation matrices: tools from random matrix theory. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0370157311001517>.
- [28] S. Abramsky and A. Brandenburger, “The sheaf-theoretic structure of non-locality and contextuality,” *New Journal of Physics*, vol. 13, no. 11, 113036, 2011. [Online]. Available: <http://dx.doi.org/10.1088/1367-2630/13/11/113036>.
- [29] A. Fine, “Hidden variables, joint probability, and the Bell inequalities,” *Phys. Rev. Lett.*, vol. 48, 291–295, 5 1982. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.48.291>.
- [30] E. Kreyszig, *Introductory functional analysis with applications*. Cambridge University Press, 1979.
- [31] K. T. Goh, J. Kaniewski, E. Wolfe, *et al.*, “Geometry of the set of quantum correlations,” *Physical Review A*, vol. 97, no. 2, 2018. [Online]. Available: <https://doi.org/10.1103/PhysRevA.97.022104>.
- [32] M. Araújo, M. T. Quintino, C. Budroni, M. T. Cunha, and A. Cabello, “All noncontextuality inequalities for the n -cycle scenario,” *Phys. Rev. A*, vol. 88, 022118, 2 2013. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.88.022118>.
- [33] A. Cabello, J. Esteban, and G. García-Alcaine, “Bell-Kochen-Specker theorem: A proof with 18 vectors,” *Physics Letters A*, vol. 212, no. 4, 183–187, 1996. [Online]. Available: [http://dx.doi.org/10.1016/0375-9601\(96\)00134-X](http://dx.doi.org/10.1016/0375-9601(96)00134-X).
- [34] S. Yu and C. H. Oh, “State-independent proof of Kochen-Specker theorem with 13 rays,” *Phys. Rev. Lett.*, vol. 108, 030402, 3 2012. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.108.030402>.
- [35] A. Peres, “Two simple proofs of the Kochen-Specker theorem,” *Journal of Physics A: Mathematical and General*, vol. 24, no. 4, L175–L178, 1991. [Online]. Available: <https://doi.org/10.1088/0305-4470/24/4/003>.
- [36] C. Okay, S. Roberts, S. D. Bartlett, and R. Raussendorf, “Topological proofs of contextuality in quantum mechanics,” 2017. [Online]. Available: <https://arxiv.org/abs/1701.01888>.
- [37] A. Peres, “Incompatible results of quantum measurements,” *Physics Letters A*, vol. 151, no. 3, 107–108, 1990. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S037596019090172K>.
- [38] N. D. Mermin, “Simple unified form for the major no-hidden-variables theorems,” *Phys. Rev. Lett.*, vol. 65, 3373–3376, 27 1990. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.65.3373>.

- [39] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Phys. Rev. Lett.*, vol. 70, 1895–1899, 13 1993. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.70.1895>.
- [40] B. Tsirelson, “Quantum analogues of the bell inequalities,” *J. Soviet Math.*, vol. 36, 557, 1987. [Online]. Available: <https://link.springer.com/article/10.1007/BF01663472>.
- [41] —, “Some results and problems on quantum bell-type inequalities,” *Hadronic J. Suppl.*, vol. 8, 329, 1993.
- [42] M. Froissart, “Constructive generalization of Bell’s inequalities,” *Il Nuovo Cimento B (1971-1996)*, vol. 64, 1981. [Online]. Available: <https://doi.org/10.1007/BF02903286>.
- [43] D. Collins and N. Gisin, “A relevant two qubit Bell inequality inequivalent to the CHSH inequality,” *Journal of Physics A: Mathematical and General*, vol. 37, no. 5, 1775–1787, 2004. [Online]. Available: <https://doi.org/10.1088%2F0305-4470%2F37%2F5%2F021>.
- [44] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, “Bell inequalities for arbitrarily high-dimensional systems,” *Phys. Rev. Lett.*, vol. 88, 040404, 4 2002. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.88.040404>.
- [45] A. Acín, R. Gill, and N. Gisin, “Optimal Bell tests do not require maximally entangled states,” *Phys. Rev. Lett.*, vol. 95, 210402, 21 2005. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.95.210402>.
- [46] J. Barrett, A. Kent, and S. Pironio, “Maximally nonlocal and monogamous quantum correlations,” *Phys. Rev. Lett.*, vol. 97, 170409, 17 2006. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.97.170409>.
- [47] J. F. Sherson, H. Krauter, R. K. Olsson, *et al.*, “Quantum teleportation between light and matter,” *Nature*, vol. 443, no. 7111, 557–560, 2006. [Online]. Available: <https://doi.org/10.1038%2Fnature05136>.
- [48] W. Pfaff, B. J. Hensen, H. Bernien, *et al.*, “Unconditional quantum teleportation between distant solid-state quantum bits,” *Science*, vol. 345, no. 6196, 532–535, 2014. [Online]. Available: <https://doi.org/10.1126%2Fscience.1253512>.
- [49] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, “Concentrating partial entanglement by local operations,” *Physical Review A*, vol. 53, no. 4, 2046–2052, 1996. [Online]. Available: <https://doi.org/10.1103%2Fphysreva.53.2046>.
- [50] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, “Purification of noisy entanglement and faithful teleportation via noisy channels,” *Physical Review Letters*, vol. 76, no. 5, 722–725, 1996. [Online]. Available: <https://doi.org/10.1103%2Fphysrevlett.76.722>.
- [51] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Reviews of Modern Physics*, vol. 74, no. 1, 145–195, 2002. [Online]. Available: <https://doi.org/10.1103%2Frevmodphys.74.145>.

- [52] R. Raussendorf and H. J. Briegel, “A one-way quantum computer,” *Phys. Rev. Lett.*, vol. 86, 5188–5191, 22 2001. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.86.5188>.
- [53] R. Raussendorf, D. E. Browne, and H. J. Briegel, “Measurement-based quantum computation on cluster states,” *Phys. Rev. A*, vol. 68, 022312, 2 2003. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.68.022312>.
- [54] L. Gutvits, “Classical deterministic complexity of edmonds problem and quantum entanglement,” ser. Proc. of the 35th ACM symp. on Theory of comp. ACM Press, 2003, 10–19.
- [55] M. Horodecki, P. Horodecki, and R. Horodecki, “Separability of mixed states: Necessary and sufficient conditions,” *Physics Letters A*, vol. 223, no. 1, 1–8, 1996. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0375960196007062>.
- [56] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement,” *Rev. Mod. Phys.*, vol. 81, 865–942, 2 2009. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.81.865>.
- [57] R. F. Werner, “Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model,” *Phys. Rev. A*, vol. 40, 4277–4281, 8 1989. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.40.4277>.
- [58] S. J. Summers and R. F. Werner, “Maximal violation of Bell’s inequalities is generic in quantum field theory,” *Commun. Math. Phys.*, vol. 110, 247, 1987. [Online]. Available: <https://link.springer.com/article/10.1007/BF01207366>.
- [59] S. Popescu and D. Rohrlich, “Which states violate Bell’s inequality maximally?” *Phys. Lett. A*, vol. 169, 411, 1992. [Online]. Available: <https://www.sciencedirect.com/science/article/abs/pii/0375960192908198?via%3Dihub>.
- [60] D. Schlingemann and R. F. Werner, “Quantum error-correcting codes associated with graphs,” *Phys. Rev. A*, vol. 65, 012308, 1 2001. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.65.012308>.
- [61] E. Hostens, J. Dehaene, and B. De Moor, “Stabilizer states and clifford operations for systems of arbitrary dimensions and modular arithmetic,” *Phys. Rev. A*, vol. 71, 042315, 4 2005. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.71.042315>.
- [62] D. Schlingemann, *Stabilizer codes can be realized as graph codes*, 2001. [Online]. Available: <https://arxiv.org/abs/quant-ph/0111080>.
- [63] K. Chen and H.-K. Lo, “Multi-partite quantum cryptographic protocols with noisy GHZ states,” 2004. [Online]. Available: <https://arxiv.org/abs/quant-ph/0404133>.
- [64] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, “Bell inequalities for graph states,” *Phys. Rev. Lett.*, vol. 95, 120405, 12 2005. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.95.120405>.
- [65] M. McKague, “Self-testing graph states,” *Conference on Quantum Computation, Communication, and Cryptography*, Springer, 2011, 104–120.
- [66] D. E. Gottesman, “Stabilizer codes and quantum error correction,” Ph.D. dissertation, California Institute of Technology, 1997.

- [67] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. V. den Nest, and H. J. Briegel, *Entanglement in graph states and its applications*, 2006. arXiv: [quant-ph/0602096](#) [quant-ph].
- [68] A. A. M. Irfan, K. Mayer, G. Ortiz, and E. Knill, “Certified quantum measurement of Majorana fermions,” *Phys. Rev. A*, vol. 101, 032106, 3 2020. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.101.032106>.
- [69] D. Mayers and A. Yao, “Self testing quantum apparatus,” 2004. arXiv: [quant-ph/0307205](#) [quant-ph].
- [70] S. Popescu and D. Rohrlich, “Which states violate Bell’s inequality maximally?” *Physics Letters A*, vol. 169, no. 6, 411–414, 1992. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/0375960192908198>.
- [71] R. Santos, D. Saha, F. Baccari, and R. Augusiak, “Scalable Bell inequalities for graph states of arbitrary prime local dimension and self-testing,” *New Journal of Physics*, 2023. [Online]. Available: <http://iopscience.iop.org/article/10.1088/1367-2630/acd9e3>.
- [72] D. Saha, R. Santos, and R. Augusiak, “Sum-of-squares decompositions for a family of noncontextuality inequalities and self-testing of quantum devices,” *Quantum*, vol. 4, 302, 2020. [Online]. Available: <https://doi.org/10.22331/2Fq-2020-08-03-302>.
- [73] R. Santos, C. Jebarathinam, and R. Augusiak, “Scalable noncontextuality inequalities and certification of multiqubit quantum systems,” *Phys. Rev. A*, vol. 106, 012431, 1 2022. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.106.012431>.
- [74] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, “Bell inequalities tailored to maximally entangled states,” *Phys. Rev. Lett.*, vol. 119, 040402, 4 2017. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.119.040402>.
- [75] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, “Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems,” *Quantum*, vol. 3, 198, Oct. 2019. [Online]. Available: <https://doi.org/10.22331/q-2019-10-24-198>.
- [76] R. Augusiak, A. Salavrakos, J. Tura, and A. Acín, “Bell inequalities tailored to the Greenberger-Horne-Zeilinger states of arbitrary local dimension,” *New Journal of Physics*, vol. 21, no. 11, 113001, 2019. [Online]. Available: <https://doi.org/10.1088/1367-2630/ab4d9f>.
- [77] K. Bharti, M. Ray, A. Varvitsiotis, A. Cabello, and L.-C. Kwek, *Local certification of programmable quantum devices of arbitrary high dimensionality*, 2019. [Online]. Available: <https://arxiv.org/abs/1911.09448>.
- [78] F. Baccari, R. Augusiak, I. Šupić, and A. Acín, “Device-independent certification of genuinely entangled subspaces,” *Phys. Rev. Lett.*, vol. 125, 260507, 26 2020. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.125.260507>.
- [79] T. Lunghi, J. B. Brask, C. C. W. Lim, *et al.*, “Self-testing quantum random number generator,” *Phys. Rev. Lett.*, vol. 114, 150501, 15 2015. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.114.150501>.

-
- [80] S.-L. Chen, C. Budroni, Y.-C. Liang, and Y.-N. Chen, “Natural framework for device-independent quantification of quantum steerability, measurement incompatibility, and self-testing,” *Phys. Rev. Lett.*, vol. 116, 240401, 24 2016. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.116.240401>.
- [81] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, “Device-independent parallel self-testing of two singlets,” *Phys. Rev. A*, vol. 93, 062121, 6 2016. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.93.062121>.
- [82] S.-L. Chen, H.-Y. Ku, W. Zhou, J. Tura, and Y.-N. Chen, “Robust self-testing of steerable quantum assemblages and its applications on device-independent quantum certification,” *Quantum*, vol. 5, 552, Sep. 2021. [Online]. Available: <https://doi.org/10.22331/q-2021-09-28-552>.
- [83] D. Wu, Q. Zhao, X.-M. Gu, *et al.*, “Robust self-testing of multiparticle entanglement,” *Phys. Rev. Lett.*, vol. 127, 230503, 23 2021. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.127.230503>.
- [84] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, “Device-independent entanglement certification of all entangled states,” *Phys. Rev. Lett.*, vol. 121, 180503, 18 2018. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.121.180503>.
- [85] B. W. Reichardt, F. Unger, and U. Vazirani, “Classical command of quantum systems via rigidity of CHSH games,” 2012. arXiv: [1209.0449](https://arxiv.org/abs/1209.0449) [quant-ph].
- [86] M. McKague, “Interactive proofs for BQP via self-tested graph states,” *Theory of Computing*, vol. 12, no. 3, 1–42, 2016. [Online]. Available: <https://theoryofcomputing.org/articles/v012a003>.
- [87] M. Markiewicz, P. Kurzyński, J. Thompson, *et al.*, “Unified approach to contextuality, nonlocality, and temporal correlations,” *Phys. Rev. A*, vol. 89, 042109, 4 2014. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.89.042109>.
- [88] M. Ardehali, “Bell inequalities with a magnitude of violation that grows exponentially with the number of particles,” *Phys. Rev. A*, vol. 46, 5375–5378, 9 1992. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.46.5375>.
- [89] N. D. Mermin, “Extreme quantum entanglement in a superposition of macroscopically distinct states,” *Phys. Rev. Lett.*, vol. 65, 1838–1840, 15 1990. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.65.1838>.
- [90] S. Pironio, A. Acín, S. Massar, *et al.*, “Random numbers certified by Bell’s theorem,” *Nature*, vol. 464, 1021, 2010. [Online]. Available: <https://www.nature.com/articles/nature09008>.
- [91] W. Helwig, “Absolutely maximally entangled qudit graph states,” 2013. [Online]. Available: <https://arxiv.org/abs/1306.2879>.

