# Robust and local quantum self-testing of systems of arbitrary high dimension 

Kishor Bharti, ${ }^{1,2, *}$ Maharshi Ray, ${ }^{2, *}$ Antonios Varvitsiotis, ${ }^{3}$ Adán Cabello, ${ }^{4,5}$ and Leong-Chuan Kwek ${ }^{2,6,7}$<br>${ }^{1}$ Institute of High Performance Computing, Agency for Science, Technology and Research ( $A^{*}$ STAR), 1 Fusionopolis Way, Connexis, Singapore 138632, Singapore<br>${ }^{2}$ Centre for Quantum Technologies, National University of Singapore<br>${ }^{3}$ Engineering Systems and Design Pillar, Singapore University of Technology and Design<br>${ }^{4}$ Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain<br>${ }^{5}$ Instituto Carlos I de Física Teórica y Computacional, Universidad de Sevilla, E-41012 Sevilla, Spain<br>${ }^{6}$ MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, Singapore UMI 3654, Singapore<br>${ }^{7}$ National Institute of Education, Nanyang Technological University, Singapore 637616, Singapore


#### Abstract

We address the problem of certifying quantum systems of arbitrary dimension (e.g., quantum computers) without making assumptions about their inner working (i.e., in a device-independent way) and without assuming that they are entangled with other systems (thus excluding self-testing methods based on violations of Bell inequalities). We show that there is a family of noncontextuality inequalities which can be expressed as a sum of probabilities of events whose graph of exclusivity is an odd antihole (i.e., the complement of a cycle with an odd number $n$ of vertices larger than three) whose maximum quantum violation is only achieved with quantum systems of dimension $d=n-2$ and is self-testable (i.e., unique up to isometries). We show that the elements of this family can be used for robust self-testing of quantum states and measurements of systems of arbitrarily high odd dimension in experiments with sequential measurements. An extra assumption needed is that measurements are ideal (i.e., minimally disturbing), which can be falsified by observation. In addition, we introduce a protocol to determine whether the quantum state and measurements maximally violating any non-contextuality inequality which can be expressed as a sum of probabilities of events is provably non-self-testable.


## I. INTRODUCTION

Classical computing devices store and manipulate sequences of binary numbers to perform computational tasks that are relevant to the society such as healthcare scheduling, weather prediction, and routing of vehicles. However, as the number of variables involved in a computational task grows beyond a limit, such as in the simulation of $50-60$ spin-half particles, even the state-of-the-art supercomputers fail spectacularly to carry out the required computations. Harnessing the properties of quantum theory to carry out computations beyond the reach of classical supercomputers is one major objective of quantum information processing. Quantum algorithms choreograph the state of a number of qubits (the quantum analogue of classical bits) in an intelligent fashion, allowing us to perform highly complex computations. Nevertheless, the ability of a quantum device to carry out a specified set of instructions relies crucially on this ability to faithfully generate on demand specific quantum states and perform specific measurements on them.

We expect future quantum resources to be shared through cloud or other internet accesses. In a faithfully minimalist scenario, developing trust in the functionality of quantum devices necessitates certification schemes that do not rely on any assumptions of their inner workings. One of the most important approaches for establishing trust in third-party quantum hardware is through the notion of self-testing [1-6]. In this setting,

[^0]the quantum device is modeled as a black box and interactions with the device correspond to measurement operations. Typical self-testing results correspond to guarantees regarding the uniqueness of the measurement settings and the underlying state preparation, based solely on the measurement statistics. The majority of existing self-testing results rely on the use of Bell inequalities, i.e., linear expressions involving probabilities of measurement-outcome events that can be carried out in a Bell experiment [7, whereas more recent works extend the self-testing paradigm beyond the scope of Bell scenarios [8, 9].

Self-testing based on Bell experiments is a powerful technique that allows us to develop insights concerning the inner workings of a pair of non-communicating entangled devices, i.e., to verify distributed quantum hardware. However, as computing typically takes place in a localized setting, any scheme for certifying the functionality of a programmable quantum computer must be of a local nature to be of any practical relevance. The first such local self-testing scheme was introduced in [10] within the framework of contextuality, which constitutes a broad generalization of Bell non-locality [7, 11. However, the contextuality-based self-testing scheme from [10] was limited in scope due to its applicability to three dimensional quantum systems. We also note the recent work [12] which investigates the possibility of a self-testing-like certification of a single untrusted quantum device. They show how a classical verifier can robustly certify that a single computationally bounded quantum prover must have prepared an EPR pair. Our main result in this article is a self-testing scheme for
local certification of programmable quantum devices of arbitrary high dimensionality.

A contextuality scenario is characterized by a set of measurement events, where two events are mutually exclusive if they correspond to the same measurement but different outcomes. The exclusivity relations between the measurement events can be conveniently encoded as edges in an undirected graph, called the exclusivity graph. The seemingly simple idea to use graphs to represent exclusivity relations has spearheaded the development of a new line of research at the interface of graph theory and contextuality [13]. The research on contextuality has led to many foundational and practical results [14-20. The linear inequalities, the violation of which witnesses contextuality, are referred to as noncontextuality inequalities. Bell inequalities are a special type of noncontextuality inequalities, where the "contexts" are provided via the space-like separation of the parties involved [7, 21]. The first "local" noncontextuality inequality violated by quantum theory was identified by Klyachko, Can, Binicioğlu, and Shumovsky (KCBS) [22]. The bound on a noncontextuality inequality in a noncontextual hidden variable (NCHV) model is called the NCHV bound. Quantum theory violates the NCHV bound for suitably chosen state and measurement settings, and thus manifests as a contextual theory. To any exclusivity graph, we associate a "canonical" noncontextuality inequality. Furthermore, we say that a graph is selftestable, if the corresponding noncontextuality inequality admits self-testing.

## II. ASSUMPTIONS AND RESULTS

Main results - The main contributions of this work can be summarized as follows:

1. We introduce a local and robust self-testing scheme for certifying high-dimensional programmable quantum devices based on contextuality. As a key ingredient in the scheme, we show that the family of odd anti-cyclic graphs with at least five vertices are self-testable. This allows for self-testing pure states and projective measurements of arbitrarily high odd dimension.
2. We present a protocol to determine whether a given graph is provably non-self-testable (see Appendix IV). This protocol goes beyond the results in Ref. [10] which only provide sufficient conditions for self-testing. We use the protocol to prove that not all graphs with a positive gap between NCHV bound and the maximum quantum bound for the corresponding canonical noncontextuality inequality admit self-testing by providing an explicit counterexample.
Assumptions- Our local certification protocol is built on four key assumptions:
3. The quantum device is programmable and is errorcorrected.
4. The measurements are ideal [23, 24], i.e.,
(a) They are outcome-replicable (give the same outcome when repeated on the same physical system).
(b) They do not disturb the compatible measurements.
(c) Their coarse-grainings also satisfy the above two properties.
5. The measurements satisfy the compatibility structure according to an odd cycle graph.
6. The device has bounded memory.

We continue with some important comments on these four assumptions. In quantum theory, ideal measurements correspond to projective measurements and the assumption that measurements are projective can be tested experimentally [25]. Some prominent examples of experiments based on ideal measurements are [26] and [27]. Moreover, any compatibility structure corresponding to a set of ideal measurements can be tested experimentally based on outcome statistics [26]. The assumption of memory is more crucial since classical simulation of the outcome statistics corresponding to contextuality experiments is possible with memory [28] 32. As every programmable device has a finite memory, the amount of memory needed to simulate the outcome statistics will get beyond the capacity of any such classical device after a certain number of rounds of the contextuality test. Determining the exact memory cost of simulating quantum contextuality corresponding to arbitrary exclusivity graphs and building an efficient (in terms of number of rounds) protocol to mitigate the memory assumption is a promising future direction. Lastly, it is important to note that our scheme is not fully device-independent because of the above assumptions. Nevertheless, a single device cannot be self-tested in a device-independent manner, so our work gives the best possible result in this setting. Our scheme is semi-device independent with experimentally testable assumptions.

## III. SELF-TESTING VIA ODD ANTI-CYCLES

Graph approach to contextuality - An arbitrary experimental scenario can be characterized by a set of measurement events $e_{1}, \ldots, e_{n}$. Two events are mutually exclusive if they correspond to same measurement but different outcomes. The exclusivity structure of a set of measurement events is captured by the exclusivity graph, denoted $\mathcal{G}_{\text {ex }}$, with nodes $\{1, \ldots, n\}$ (denoted by $[n])$ corresponding to events $\left\{e_{i}\right\}_{i=1}^{n}$. Two nodes $i$ and $j$ are adjacent (denoted by $i \sim j$ ) if $e_{i}$ and $e_{j}$ are mutually exclusive.

Given an experimental scenario with an exclusivity graph $\mathcal{G}_{\text {ex }}$, a theory assigns probability to the events corresponding to its vertices. The mapping $p:[n] \rightarrow$ $[0,1]$, where $p_{i}+p_{j} \leq 1$, for all $i \sim j$ is called a behavior. Here, the non-negative numbers $p_{i}$ refer to the probability of the event $e_{i}$. We call a behavior $p$ deterministic noncontextual if all the probabilities $p_{i}$ are either 0 or 1 and the occurrence of a event does not depend on the possibility of occurrence of other events. The convex hull of all deterministic noncontextual behaviors forms a polytope, denoted by $\mathcal{P}_{n c}\left(\mathcal{G}_{\text {ex }}\right)$, which contains all possible noncontextual behaviors for the experimental scenario encoded by the graph $\mathcal{G}_{\text {ex }}$. The behaviors which lie outside $\mathcal{P}_{n c}\left(\mathcal{G}_{\text {ex }}\right)$ are contextual behaviors. The set of noncontextual behaviors is bounded by finitely many half spaces, which are called noncontextuality inequalities. Formally speaking, noncontextuality inequalities correspond to linear inequalities of the form

$$
\begin{equation*}
\sum_{i \in[n]} w_{i} p_{i} \leq B_{n c}\left(\mathcal{G}_{\mathrm{ex}}, w\right), \forall p \in \mathcal{P}_{n c}\left(\mathcal{G}_{\mathrm{ex}}\right) \tag{1}
\end{equation*}
$$

where $w_{1}, \ldots, w_{n} \geq 0$ and $B_{n c}\left(\mathcal{G}_{\text {ex }}, w\right)$ are real scalars. The noncontextuality inequalities with all the weights $\left\{w_{i} \mathrm{~s}\right\}$ equal to one will be referred to as canonical noncontextuality inequalities. By definition, $B_{n c}\left(\mathcal{G}_{\text {ex }}, w\right)$ corresponds to the NCHV bound on the linear expression $\sum_{i \in[n]} w_{i} p_{i}$ and is also equal to the weighted independence number of the exclusivity graph $\mathcal{G}_{\text {ex }}$, defined as the cardinality of the largest set of pairwise non-adjacent nodes of $\mathcal{G}_{\text {ex }}$ [13]. A quantum behavior has the following form:

$$
\begin{equation*}
p_{i}=\operatorname{tr}\left(\rho \Pi_{i}\right), \forall i \in[n] \text { and } \operatorname{tr}\left(\Pi_{i} \Pi_{j}\right)=0, \text { for } i \sim j \tag{2}
\end{equation*}
$$

for some quantum state $\rho$ and quantum projectors $\Pi_{1}, \ldots, \Pi_{n}$ acting on a Hilbert space $\mathcal{H}$. An ensemble $\rho,\{\Pi\}_{i=1}^{n}$ satisfying (2) is called a quantum realisation of the behavior $p$. For a given quantum behavior $p$, there can be multiple quantum realisations. The set of quantum behaviors is a convex set, which we denote by $\mathcal{P}_{q}\left(\mathcal{G}_{\text {ex }}\right)$. The maximum value of the linear expression $\sum_{i \in[n]} w_{i} p_{i}$, as $p$ ranges over the set of quantum behaviors, $\mathcal{P}_{q}\left(\mathcal{G}_{\text {ex }}\right)$ can exceed the classical bound. We will denote the maximum attainable quantum value by $B_{c q}\left(\mathcal{G}_{\mathrm{ex}}, w\right)$. Interestingly, $B_{c q}\left(\mathcal{G}_{\mathrm{ex}}, w\right)$ is equal to the Lovász theta number of the graph $\mathcal{G}_{\text {ex }}$ and admits a formulation as a tractable optimisation problem known as a semidefinite program [13] (see Methods Section).
Robust self-testing - Informally speaking, a noncontextuality inequality $\mathcal{I}$ is said to self-test a quantum realisation $\rho,\{\Pi\}_{i=1}^{n}$ if it achieves the quantum bound for the noncontextuality inequality $\mathcal{I}$ and furthermore, all other quantum realisations which achieve the quantum bound corresponding to $\mathcal{I}$ are equivalent to $\rho,\{\Pi\}_{i=1}^{n}$ up to global isometry. For a formal definition, the reader is referred to

Section B in the Appendix. As discussed in [10, the essential ingredient in proving self-testing results for a noncontextuality inequality $\mathcal{I}$ with underlying exclusivity graph $\mathcal{G}_{\text {ex }}$ is that the corresponding Lovász theta semidefinite program (cf. $P_{G}$ ) has an unique optimal solution. In the case of the KCBS inequality, the exclusivity graph is a pentagon. The configuration corresponding to optimal quantum violation admits an umbrella structure. The KCBS inequality has been generalized to odd $n$-cycle exclusivity graphs, which are called $\mathrm{KCBS}_{\mathrm{n}}$ inequalities. The $\mathrm{KCBS}_{\mathrm{n}}$ inequalities are the canonical nonconcontextuality inequalities for an odd cycle graph and admit robust self-testing [10].

Self-testing anti-cycles - Building on the link between graph theory and contextuality [33], in combination with the strong perfect graph theorem [34], it was shown in [13, [33] that the presence of certain exclusivity structures is a necessary and sufficient condition for a noncontextuality scenario to witness quantum contextuality. These fundamental exclusivity structures correspond to an odd number of events that are either cyclically or anticyclically exclusive. In the graph theory literature, odd cycles and odd anti-cycles are called odd holes and odd antiholes respectively. The canonical noncontextuality inequality for an antihole is given by:

$$
\begin{equation*}
\sum_{i=1}^{n} p_{i} \leq 2, \quad \text { for all } p \in \mathcal{P}_{n c}\left(\overline{C_{n}}\right) \tag{3}
\end{equation*}
$$

which we call antihole inequalities and correspond to facets of the classical polytope for $\overline{C_{n}}$. The quantum bound for the antihole inequalities, i.e., the Lovász theta number for $\overline{C_{n}}$ is $\frac{1+\cos \frac{\pi}{n}}{\cos \frac{\pi}{n}}$. A canonical quantum ensemble which achieves the quantum value for the antihole inequalities corresponding to odd $n$ is given by $n-2$ dimensional quantum state and projectors. In fact the dimension of quantum system achieving optimal quantum violation of antihole inequalities must be $n-2$ for odd $n$. We provide a proof of the aforementioned claim in Appendix D. Moreover, we show that the antihole inequalities admit robust self-testing. This fact is proven in the Appendix (Sections B and C).

As the presence of holes and/or antiholes in a contextuality scenario dictates the possibility of quantum advantage [33], our result regarding antihole self-testing in combination with [10] imply that all noncontextuality inequalities which are fundamental to quantum theory admit local robust self-testing. This is because the generalized KCBS and antihole inequalities are the unique facet-defining noncontextuality inequalities for their respective odd hole and antihole exclusivity scenarios [35].

## IV. NOT ALL NONCONTEXTUALITY INEQUALITIES ADMIT SELF-TESTING

We have proved that all fundamental noncontextuality inequalities admit self-testing. A natural question is whether every noncontextuality inequality with separation between corresponding noncontextual hidden variable bound and quantum bound admits self-testing. Below we provide an explicit noncontextuality inequality which shows that the answer is negative. In graph theoretical terms, we identify a non-perfect graph whose Lovász theta SDP admits multiple primal optimal solutions. We make crucial use of the following result [36, Theorem 5] to determine the (non)uniqueness of primal optimal under strict complementarity, see also [37].

Theorem 1. Let $\left(X^{*}, Z^{*}\right)$ be a pair of primal and dual optimal solutions satisfying strict complementarity. Then, uniqueness of $X^{*}$ implies that $Z^{*}$ is dual nondegenerate.

The exclusivity graph of our counter-example is shown in Figure 1. The corresponding canonical noncontextuality inequality is given by

$$
\begin{equation*}
\sum_{i=1}^{6} p_{i} \leq 2 \tag{4}
\end{equation*}
$$

whose quantum bound is equal to $\sqrt{5}$.


FIG. 1. The above exclusivity graph corresponds to the canonical noncontextuality inequality with minimal number of measurement events which doesn't admit self-testing.

Consider the pair of primal-dual optimal solutions

$$
Z^{\star}=\left[\begin{array}{c|cccccc}
\sqrt{5} & -1 & -1 & -1 & -1 & -1 & -1 \\
\hline-1 & 1 & 0 & c & c & 0 & c \\
-1 & 0 & 1 & 0 & c & c & c \\
-1 & c & 0 & 1 & 0 & c & 0 \\
-1 & c & c & 0 & 1 & 0 & 1 \\
-1 & 0 & c & c & 0 & 1 & 0 \\
-1 & c & c & 0 & 1 & 0 & 1
\end{array}\right]
$$

where $c=\frac{\sqrt{5}-1}{2}$ and

$$
X^{\star}=\left[\begin{array}{c|cccccc}
1 & f & f & f & h & f & h  \tag{6}\\
\hline f & f & k & 0 & 0 & k & 0 \\
f & k & f & k & 0 & 0 & 0 \\
f & 0 & k & f & r & 0 & r \\
h & 0 & 0 & r & h & r & 0 \\
f & k & 0 & 0 & r & f & r \\
h & 0 & 0 & r & 0 & r & h
\end{array}\right]
$$

where $f=\frac{1}{\sqrt{5}}, h=\frac{f}{2}, k=\frac{5-\sqrt{5}}{10}$ and $r=\frac{k}{2}$. Since $\operatorname{rank}\left(Z^{*}\right)=3$ and $\operatorname{rank}(X)^{\star}=4$, strict complementarity holds. Using Theorem 11 the uniqueness of $X^{*}$ implies dual nondegeneracy. To determine dual nondegeneracy for $Z^{*}$ we (once again) resort to solving a system of linear equations. The symmetric variable matrix $M$ is given by

$$
M=\left[\begin{array}{c|cccccc}
0 & m_{0} & m_{1} & m_{2} & m_{3} & m_{4} & m_{5}  \tag{7}\\
\hline m_{0} & m_{0} & m_{6} & 0 & 0 & m_{7} & 0 \\
m_{1} & m_{6} & m_{1} & m_{8} & 0 & 0 & 0 \\
m_{2} & 0 & m_{8} & m_{2} & m_{9} & 0 & m_{10} \\
m_{3} & 0 & 0 & m_{9} & m_{3} & m_{11} & 0 \\
m_{4} & m_{7} & 0 & 0 & m_{11} & m_{4} & m_{12} \\
m_{5} & 0 & 0 & m_{10} & 0 & m_{12} & m_{5}
\end{array}\right]
$$

Solving for the linear systems of equations $Z^{\star} M=0$, we get $m_{11}=-m_{12}, m_{10}=m_{12}, m_{5}=\frac{1+\sqrt{5}}{2} m_{12}$, $m_{9}=-m_{12}, m_{3}=-\left(\frac{1+\sqrt{5}}{2}\right) m_{12}, m_{0}=m_{1}=m_{2}=$ $m_{4}=m_{6}=m_{7}=m_{8}=0$. For example, if we set $m_{12}=1$, we can get a consistent assignment of $m_{i}$, from $i=0$ to 12 , which isn't all zero. Hence, the dual solution $Z^{*}$ is degenerate, which together with strict complementarity implies that the primal is not unique. Thus the noncontextuality inequality in (4) does not admit self-testing.

We also report that we found several other non-perfect graphs ( equivalently noncontextuality inequalities) which do not admit self-testing. Identifying the exact classes of graphs which admit self-testing will be interesting but we leave that as an open question.

## V. TOOLS AND TECHNIQUES

The main tool we use in this work to show that antihole inequalities admit robust self-testing is Theorem 2, shown in [10], which provides a sufficient condition for a graph to be self-testable. This result relies crucially on the rich properties of a powerful class of mathematical optimisation models, known as Semidefinite programs (SDPs) (see Appendix A). SDPs constitute a vast generalisation of linear optimisation models where scalar variables are replaced by vectors and the constraints and objective function are affine in terms of the inner products of the vectors. Equivalently, collecting all pairwise inner products of these vectors in matrix, known as the Gram matrix, an SDP corresponds to optimising a linear function of the Gram matrix subject
to affine constraints. Analogously to linear programs, to any SDP there is an associated a dual program whose value is equal to the primal under reasonable assumptions. Next, we single out certain properties of primal-dual solutions that are of relevance to his work. A pair of primal dual optimal solutions $\left(X^{*}, Z^{*}\right)$ with no duality gap (i.e., $\operatorname{tr}\left(X^{*} Z^{*}\right)=0$ ), satisfies strict complementarity if the Range ( $X^{*}$ ) and Range $\left(Z^{*}\right)$ give a direct sum decomposition of the underlying space. Furthermore, an optimal dual solution $Z^{*}$ with rank $r$ is dual nondegenerate if the tangent space at $Z^{*}$ of the manifold of symmetric matrices with rank equal to $r$ together with the linear space of matrices defining the SDP span the entire space of symmetric matrices. In this work we focus on the Lovász theta SDP, see $\left(P_{G}\right)$ in Appendix B. The proof of our main result involves two main steps. First, we construct a dual optimal solution of $D_{G}$ for an odd-cycle graph by providing an explicit mapping between the Gram vectors of a primal $P_{G}$ optimal solution of an odd-cycle graph and the Gram vectors of a dual optimal solution of the complement graph; see Theorem 3 for details. Next, once we construct a dual optimal solution, we show in Theorem 4 that it satisfies the non-degeneracy conditions given in (B4). By Theorem 2, this shows that antihole inequalities admit robust self-testing. Details of the proofs can be found in Appendix C. Additionally, we show that not all graphs admit self-testing by providing a counter example of such a graph (see Appendix IV]. The overall scheme for determining whether a graph is self-testable (equivalently whether the primal optimal solution of the Lovász theta SDP corresponding to that graph is unique or not) is provided in the form of a flowchart in Figure 2

## VI. OPEN PROBLEMS

We proceed with some mathematical questions of physical relevance that are raised by our work. First, the dimension of the quantum system corresponding to the maximum quantum violation of a noncontextuality inequality is given by the rank of the corresponding primal optimal matrix of the semidefinite program. In this work we proved that the dimension of the quantum system must be at least $n-2$, which corresponds to the maximum violation of the anti-cycle inequality with $n$ vertices in its exclusivity graph. To make our analysis robust with respect to experimental errors, it is important to identify lower bounds on the dimension of the quantum system when we tolerate $\epsilon$-suboptimal solutions.

Second, the outcome statistics corresponding to contextuality experiments can be classically simulated using memory. As discussed above, one way to mitigate this is to run the contextuality tests for sufficiently large number of rounds so that the programmable device runs out of memory. One future direction will be to determine the exact memory cost of simulating


FIG. 2. Flowchart for determining (non)uniqueness of primal solution(s). Here inconclusive* refers to the fact that one can still hope to arrive at a definitive answer by restarting the algorithm using a different dual optimal solution (if it exists).
quantum contextuality corresponding to arbitrary exclusivity graphs. Estimating the memory cost of simulating contextuality is comparatively easier for state-independent scenarios. It will be interesting to develop self-testing schemes for measurement settings corresponding to state-independent noncontextuality inequalities. Another exciting direction would be to explore if it's possible to prevent the prover from classically simulating the output statistics using cryptographic tools, such as blind quantum computing [38]. This will also ensure that the protocol is efficient in terms of the number of testing rounds.

Third, the noise robustness of a noncontextuality inequality can be quantified by the ratio of the corresponding quantum bound $\vartheta\left(\mathcal{G}_{\text {ex }}, w\right)$ to the classical bound $\alpha\left(\mathcal{G}_{\text {ex }}, w\right)$. For anti-cycle inequalities, the ratio tends to one, and thus the self-testing scheme is not noise-tolerant. However, there are graphs for which the quantum to classical ratio scales with the number of vertices of the underlying exclusivity graph [39]. It will be exciting to provide self-testing schemes for such noisetolerant graphs, as this could be used to self test NISQ devices.

## VII. ACKNOWLEDGEMENTS

We thank the National Research Foundation of Singapore, the Ministry of Education of Singapore, MINECO Project No. FIS2017-89609-P with FEDER funds, and the Knut and Alice Wallenberg Foundation for financial support. A significant part of the research project Local certification of programmable quantum devices of arbitrary high dimensionalitywas carried out during "New directions in quantum information" conference organized by Nordita, the Nordic Institute for Theoretical Physics.

## APPENDIX

## Appendix A: Semidefinite programming basics

A semidefinite program (SDP) is given by an optimisation problem of the following form

$$
\begin{equation*}
\sup _{X}\left\{\langle C, X\rangle: X \in \mathcal{S}_{+}^{n},\left\langle A_{i}, X\right\rangle=b_{i}(i \in[m])\right\} \tag{P}
\end{equation*}
$$

where $\mathcal{S}_{+}^{n}$ denotes the cone of $n \times n$ real positive semidefinite matrices and $\langle X, Y\rangle=\operatorname{tr}\left(X^{T} Y\right)$. The corresponding dual problem is given by

$$
\begin{equation*}
\inf _{y, Z}\left\{\sum_{i=1}^{m} b_{i} y_{i}: \sum_{i=1}^{m} y_{i} A_{i}-C=Z \in \mathcal{S}_{+}^{n}\right\} \tag{D}
\end{equation*}
$$

A pair of primal-dual optimal solutions $\left(X^{*}, Z^{*}\right)$ with no duality gap (i.e., $\operatorname{tr}\left(X^{*} Z^{*}\right)=0$ ), satisfies strict complementarity if

$$
\begin{equation*}
\operatorname{rank}\left(X^{*}\right)+\operatorname{rank}\left(Z^{*}\right)=n . \tag{A1}
\end{equation*}
$$

Lastly, an optimal dual solution $Z^{*}$ is called dual nondegenerate if the linear system in the symmetric matrix variable $M$

$$
\begin{equation*}
M Z^{*}=\operatorname{tr}\left(M A_{1}\right)=\ldots=\operatorname{tr}\left(M A_{m}\right)=0 \tag{A2}
\end{equation*}
$$

only admits the trivial solution $M=0$.
Central to this work is the Lovász theta SDP corresponding to a graph $G$, whose primal formulation is:

$$
\begin{align*}
\vartheta(G)=\max & \sum_{i=1}^{n} X_{i i} \\
\text { s.t. } & X_{i i}=X_{0 i}, i \in[n]  \tag{G}\\
& X_{i j}=0, i \sim j \\
& X_{00}=1, \quad X \in \mathcal{S}_{+}^{1+n}
\end{align*}
$$

and the dual formulation we use is given by:

$$
\begin{aligned}
\vartheta(G)=\min & Z_{00} \\
\text { s.t. } & Z_{i i}=-\left(2 Z_{0 i}+1\right), i \in[n] \\
& Z_{i j}=0, i \nsim j \\
& Z \in \mathcal{S}_{+}^{1+n}
\end{aligned}
$$

## Appendix B: Robust self-testing

To prove our main result we use the following definitions from [10]. A noncontextuality inequality $\sum_{i \in[n]} w_{i} p_{i} \leq B_{n c}\left(\mathcal{G}_{\text {ex }}, w\right)$ is a self-test for the realisation $\left\{\left|u_{i}\right\rangle\left\langle u_{i}\right|\right\}_{i=0}^{n}$ if:

1. $\left\{\left|u_{i}\right\rangle\left\langle u_{i}\right|\right\}_{i=0}^{n}$ achieves the quantum supremum $B_{q c}\left(\mathcal{G}_{\text {ex }}, w\right)$;
2. For any other realisation $\left\{\left|u_{i}^{\prime}\right\rangle\left\langle u_{i}^{\prime}\right|\right\}_{i=0}^{n}$ that also achieves $B_{q c}\left(\mathcal{G}_{\text {ex }}, w\right)$, there exists an isometry $V$ such that

$$
\begin{equation*}
V\left|u_{i}\right\rangle\left\langle u_{i}\right| V^{\dagger}=\left|u_{i}^{\prime}\right\rangle\left\langle u_{i}^{\prime}\right|, \quad 0 \leq i \leq n \tag{B1}
\end{equation*}
$$

Furthermore, a noncontextuality inequality $\sum_{i \in[n]} w_{i} p_{i} \leq B_{n c}\left(\mathcal{G}_{\text {ex }}, w\right)$ is an $(\epsilon, r)$-robust selftest for $\left\{\left|u_{i}\right\rangle\left\langle u_{i}\right|\right\}_{i=0}^{n}$ if it is a self-test, and furthermore, for any other realisation $\left\{\left|u_{i}^{\prime}\right\rangle\left\langle u_{i}^{\prime}\right|\right\}_{i=0}^{n}$ satisfying

$$
\sum_{i=1}^{n} w_{i}\left|\left\langle u_{i}^{\prime} \mid u_{0}^{\prime}\right\rangle\right|^{2} \geq B_{q c}\left(\mathcal{G}_{\mathrm{ex}}, w\right)-\epsilon
$$

there exists an isometry $V$ such that

$$
\begin{equation*}
\| V\left|u_{i}\right\rangle\left\langle u_{i}\right| V^{\dagger}-\left|u_{i}^{\prime}\right\rangle\left\langle u_{i}^{\prime}\right| \| \leq \mathcal{O}\left(\epsilon^{r}\right), \quad 0 \leq i \leq n \tag{B2}
\end{equation*}
$$

The proof of our main result hinges on the following theorem (first introduced in [10]):

Theorem 2. Consider a noncontextuality inequality $\sum_{i=1}^{n} w_{i} p_{i} \leq B_{n c}\left(\mathcal{G}_{\text {ex }}, w\right)$. Assume that

1. There exists an optimal quantum realisation $\left\{\left|u_{i}\right\rangle\left\langle u_{i}\right|\right\}_{i=0}^{n}$ such that

$$
\begin{equation*}
\sum_{i} w_{i}\left|\left\langle u_{i} \mid u_{0}\right\rangle\right|^{2}=B_{q c}\left(\mathcal{G}_{\mathrm{ex}}, w\right) \tag{B3}
\end{equation*}
$$

and $\left\langle u_{0} \mid u_{i}\right\rangle \neq 0$, for all $1 \leq i \leq n$, and
2. There exists a dual optimal solution $Z^{*}$ for the SDP ( $D_{G}$ ) such that the homogeneous linear system

$$
\begin{align*}
M_{0 i} & =M_{i i}, \text { for all } 1 \leq i \leq n \\
M_{i j} & =0, \text { for all } i \sim j  \tag{B4}\\
M Z^{*} & =0
\end{align*}
$$

in the symmetric matrix variable $M$ only admits the trivial solution $M=0$.

Then, the noncontextuality inequality is an $\left(\epsilon, \frac{1}{2}\right)$-robust self-test for $\left\{\left|u_{i}\right\rangle\left\langle u_{i}\right|\right\}_{i=0}^{n}$.

## Appendix C: Self-testing antihole inequalities

The antihole noncontextuality inequalities are given by $\sum_{i=1}^{n} p_{i} \leq 2$ for all $p \in \mathcal{P}_{n c}\left(\overline{C_{n}}\right)$. The quantum
bound for the antihole inequalities, i.e., the Lovász theta number for $\overline{C_{n}}$ is $\frac{1+\cos \frac{\pi}{n}}{\cos \frac{\pi}{n}}$ [40]. A canonical quantum ensemble which achieves the quantum value for the antihole inequalities corresponding to odd $n$ is given by $n-2$ dimensional quantum state and projectors. Explicitly, the quantum state is

$$
\begin{equation*}
\left|v_{0}\right\rangle=(1,0, \ldots, 0)^{T} \tag{C1}
\end{equation*}
$$

but the description of the projectors $\left\{\Pi_{j}=\left|v_{j}\right\rangle\left\langle v_{j}\right|\right\}_{j=1}^{n}$ is more involved [33]. Let us denote the $k$-th component of $\left|v_{j}\right\rangle$ corresponding to projector $\Pi_{j}$ as $v_{j, k}$. For $0 \leq j \leq n-1$ and $0 \leq k \leq n-3$,

$$
\begin{align*}
v_{j, 0} & =\sqrt{\frac{\vartheta\left(\overline{C_{n}}\right)}{n}}  \tag{C2}\\
v_{j, 2 m-1} & =T_{j, m} \cos R_{j, m}  \tag{C3}\\
v_{j, 2 m} & =T_{j, m} \sin R_{j, m} \tag{C4}
\end{align*}
$$

for $m=1,2, \ldots \frac{n-3}{2}$ and

$$
\begin{gather*}
T_{j, m}=(-1)^{j(m+1)} \sqrt{\frac{2 \cos \left(\frac{\pi}{n}\right)+(-1)^{m+1} \cos \left(\frac{(m+1) \pi}{n}\right)}{n \cos \frac{\pi}{n}}},  \tag{C5}\\
R_{j, m}=\frac{j(m+1) \pi}{n} . \tag{C6}
\end{gather*}
$$

For the antihole noncontextuality inequalities, the ensemble described above achieves the quantum value and satisfies the first condition of Theorem 2. It remains to establish the existence of a dual optimal solution for the SDP corresponding to the Lovász theta number of antihole graphs such that the conditions in (B4) are satisfied. Towards this goal, we first proceed to provide the explicit form of the dual optimal solution.

Theorem 3. Let $X^{*}=\operatorname{Gram}\left(v_{0}, v_{1}, \ldots, v_{n}\right)$ be the unique optimal solution for $\left(P_{C_{n}}\right)$. Then,

$$
\begin{equation*}
Z_{n}^{*}=\vartheta\left(\overline{C_{n}}\right) \operatorname{Gram}\left(-v_{0}, v_{1}, \ldots, v_{n}\right) \tag{C7}
\end{equation*}
$$

is a dual optimal solution for $\left(D_{\overline{C_{n}}}\right)$. Another useful expression for $Z_{n}^{*}$ is given by

$$
Z_{n}^{\star}=\left[\begin{array}{c|c}
\vartheta\left(\overline{C_{n}}\right) & -e^{\top}  \tag{C8}\\
\hline-e & \operatorname{circ}(u)
\end{array}\right] \in \mathbb{R}^{(1+n) \times(1+n)}
$$

where $e$ is the vector of all ones of length $n$,

$$
\begin{equation*}
u=\left(1, \vartheta\left(\overline{C_{n}}\right)\left\langle v_{1} \mid v_{2}\right\rangle, \ldots, \vartheta\left(\overline{C_{n}}\right)\left\langle v_{1} \mid v_{n}\right\rangle\right), \tag{C9}
\end{equation*}
$$

and $\operatorname{circ}(\cdot)$ maps an $n$-dimensional vector and outputs the corresponding circulant matrix.

Proof. It was shown in [10] that $\left(P_{C_{n}}\right)$ admits a unique optimal solution $X^{*}$. For any $k=0,1, \ldots, n-1$, the map taking $i \rightarrow i+1$ (modulo $n$ ) is an automorphism of $C_{n}$ (i.e., a bijective map that preserves adjacency and non-adjacency). In particular, this implies that $X^{*}$ is circulant and furthermore, constant along each band. Specifically, all diagonal entries of $X^{*}$ are equal, and as $\vartheta\left(C_{n}\right)=\sum_{i=1} X_{i i}^{*}$, it follows that

$$
\begin{equation*}
\left\langle v_{i} \mid v_{i}\right\rangle=X_{i i}^{*}=\vartheta\left(C_{n}\right) / n \tag{C10}
\end{equation*}
$$

Analogously, for a pair of indices $i, j$ with $|i-j|=k$ we have that $X_{i j}^{*}=\left\langle v_{1} \mid v_{k+1}\right\rangle$. Moreover, the feasibility of $X^{*}$ we have that $X_{00}^{*}=\left\langle v_{0} \mid v_{0}\right\rangle=1$. Thus $Z_{00}^{*}=\vartheta\left(\overline{C_{n}}\right)$ has the correct value and it remains to show that $Z^{*}$ is feasible. Next, by feasibility of $X^{*}$ we have that $X_{i j}^{*}=$ $\left\langle v_{i} \mid v_{j}\right\rangle=0$, when $i \sim j$ in $C_{n}$. Thus, by definition of $Z^{*}$ we have that $Z_{i j}^{*}=\vartheta\left(\overline{C_{n}}\right)\left\langle v_{i} \mid v_{j}\right\rangle=0$ for all edges of $C_{n}$. Finally we show that $Z_{i i}^{*}=-\left(2 Z_{0 i}^{*}+1\right), i \in[n]$. Indeed,

$$
\begin{equation*}
Z_{i i}^{*}=\left\langle v_{i} \mid v_{i}\right\rangle \vartheta\left(\overline{C_{n}}\right)=\frac{\vartheta\left(C_{n}\right)}{n} \vartheta\left(\overline{C_{n}}\right)=1 \tag{C11}
\end{equation*}
$$

where we used (C10) and that $\vartheta\left(C_{n}\right) \vartheta\left(\overline{C_{n}}\right)=n$ (see Theorem 8 of 41]). To finish the proof we note that

$$
\begin{align*}
-\left(2 Z_{0 i}^{*}+1\right) & =-\left(2 \vartheta\left(\overline{C_{n}}\right)\left\langle-v_{0} \mid v_{i}\right\rangle+1\right) \\
& =2 \vartheta\left(\overline{C_{n}}\right)\left\langle v_{0} \mid v_{i}\right\rangle-1  \tag{C12}\\
& =2 \vartheta\left(\overline{C_{n}}\right)\left\langle v_{i} \mid v_{i}\right\rangle-1 \\
& =1
\end{align*}
$$

where the second last equality follows from the constraint that $\left\langle v_{0} \mid v_{i}\right\rangle=\left\langle v_{i} \mid v_{i}\right\rangle$ for $i \in[n]$ and the last equality follows by substituting $\left\langle v_{i} \mid v_{i}\right\rangle \vartheta\left(\overline{C_{n}}\right)=1$.

Finally, we show that the dual optimal solution satisfies the conditions in B4.

Theorem 4. The dual optimal solution $Z^{*}$ corresponding to the complement of an odd-cycle graph satisfies the conditions in B4.

Proof. We show that for any odd $n$, the only symmetric matrix $M \in \mathbb{R}^{(1+n) \times(1+n)}$ satisfying

$$
\begin{equation*}
M_{00}=0, M_{0 i}=M_{i i}, M_{i j}=0(\forall i \sim j), M Z^{*}=0 \tag{C13}
\end{equation*}
$$

is the matrix $M=0$, where $i \sim j$ here refers to an edge in the $\overline{C_{n}}$ graph. Barring the $M Z^{*}=0$ constraint, the rest already guarantee that there are at most $2 n$ potentially non-zero entries in the $M$ matrix (not counting the repeated entries) corresponding to $\overline{C_{n}}$ graph. Let the first row of $M$ be $\left(0, m_{1}, m_{2}, \ldots, m_{n}\right)$. We fill the rest of the potential non-zero slots in $M$ with $m_{n+1}, m_{n+2}, \ldots, m_{2 n}$.

For example, for $n=7$, we have

$$
M_{7}=\left(\begin{array}{c|ccccccc}
0 & m_{1} & m_{2} & m_{3} & m_{4} & m_{5} & m_{6} & m_{7}  \tag{C14}\\
\hline m_{1} & m_{1} & m_{8} & 0 & 0 & 0 & 0 & m_{14} \\
m_{2} & m_{8} & m_{2} & m_{9} & 0 & 0 & 0 & 0 \\
m_{3} & 0 & m_{9} & m_{3} & m_{10} & 0 & 0 & 0 \\
m_{4} & 0 & 0 & m_{10} & m_{4} & m_{11} & 0 & 0 \\
m_{5} & 0 & 0 & 0 & m_{11} & m_{5} & m_{12} & 0 \\
m_{6} & 0 & 0 & 0 & 0 & m_{12} & m_{6} & m_{13} \\
m_{7} & m_{14} & 0 & 0 & 0 & 0 & m_{13} & m_{7}
\end{array}\right),
$$

For notational convenience, let $M Z^{*}=\left(\begin{array}{cc}q & r^{\top} \\ r & T\end{array}\right)$, where $T \in \mathbb{R}^{n \times n}, q \in \mathbb{R}$ and $r \in \mathbb{R}^{n \times 1}$. In the rest of this section we use the notation $\underline{i}$ to denote $i \bmod n$, where $i$ is an integer. The linear equation corresponding to $q$ implies that

$$
\begin{equation*}
\sum_{i=1}^{n} m_{i}=0 \tag{C15}
\end{equation*}
$$

For $i \in\{1,2, \ldots, n\}$, the $2 n$ linear equations corresponding to $T_{i, \underline{i+1}}$ and $T_{i, \underline{i-1}}$ imply

$$
\begin{equation*}
m_{n+1}=m_{n+2}=\ldots=m_{2 n} \tag{C16}
\end{equation*}
$$

Now consider the $n$ linear equations corresponding to $r$. These equations along with C16 imply

$$
\begin{equation*}
m_{1}=m_{2}=\ldots=m_{n} \tag{C17}
\end{equation*}
$$

Using C17 along with C15 we have

$$
\begin{equation*}
m_{1}=m_{2}=\ldots=m_{n}=0 \tag{C18}
\end{equation*}
$$

Finally, using the equations corresponding to $r$ again and C18 we have

$$
\begin{equation*}
m_{n+1}=m_{n+2}=\ldots=m_{2 n}=0 \tag{C19}
\end{equation*}
$$

implying that $M=0$, as desired.

## Appendix D: Dimension for optimal violation of antihole inequalities

Theorem 5. Given an antihole noncontextuality inequality with an odd number of $n$ measurement events, the quantum system achieving the optimal quantum bound must be at least $(n-2)$ dimensional.

Proof. The value of a noncontextuality inequality achievable within quantum theory is equal to the weighted Lovász theta number of the underlying graph $G$ and admits the SDP formulation $\left(\overline{P_{G}}\right)$. The lower bound on the dimension of a quantum system achieving the optimal quantum bound is the rank of the unique primal optimal matrix

$$
X_{n}^{\star}=\left[\begin{array}{c|c}
1 & \frac{\vartheta\left(\overline{C_{n}}\right)}{n} e^{\top}  \tag{D1}\\
\hline \frac{v\left(\overline{C_{n}}\right)}{n} e & \operatorname{circ}(u)
\end{array}\right]
$$

where $e$ is the all-ones vector of length $n, \operatorname{circ}(\cdot)$ is the circulant function that takes as input a $n$ dimension vector and outputs a $n \times n$ matrix with the input vector as its top row and every subsequent row being one place right shifted modulo $n$ and $u=$ $\left(\frac{\vartheta\left(\overline{C_{n}}\right)}{n}, \frac{n-\vartheta\left(C_{n}\right)}{2 \vartheta\left(C_{n}\right)^{2}}, 0,0,0, \ldots, 0,0, \frac{n-\vartheta\left(C_{n}\right)}{2 \vartheta\left(C_{n}\right)^{2}}\right)$. Since $X_{n}^{\star}$ is real, its rank over complex field is the same as over real field and equals to the number of nonzero eigenvalues (with multiplicity). Furthermore, a lower bound on the rank of $X_{n}^{\star}$ is given by the rank of the lower right block matrix (the circulant portion). The eigenvalues of a circulant matrix can be calculated easily using the circulant vector. A few lines of algebra yields the following expression for the eigenvalues of the lower right block matrix,

$$
\begin{equation*}
\lambda_{j}=\frac{1}{\vartheta_{n}}+\frac{n-\vartheta_{n}}{\vartheta_{n}} \cos \left(\frac{2 \pi j}{n}\right) \tag{D2}
\end{equation*}
$$

for $j \in[n]$ and $\vartheta_{n}$ denotes the Lovász theta number for the holes with odd $n$. One can see that $\lambda_{j} \neq 0$ unless $j=\frac{n-1}{2}$ or $\frac{n+1}{2}$. Thus, the rank of the circulant matrix is $n-2$ for all odd values of $n$. Thus, the lower bound on the rank of the optimal feasible matrix $X^{\star}$ is $n-2$ which is same as the lower bound on the dimension of the desired quantum system.

## Appendix E: Complex versus Real SDPs

Lemma 6. Consider a real SDP

$$
\begin{equation*}
\sup _{X}\left\{\langle C, X\rangle: X \in \mathcal{S}_{+}^{n},\left\langle A_{i}, X\right\rangle=b_{i}(i \in[m])\right\} \tag{E1}
\end{equation*}
$$

that admits a unique optimal solution $X^{*}$ witnessed by a dual nondegenerate optimal solution $Z^{*}$. Then, the SDP considered over the complex numbers, i.e.,

$$
\begin{equation*}
\sup _{X}\left\{\langle C, X\rangle_{\mathbb{C}}: X \in \mathcal{H}_{+}^{n},\left\langle A_{i}, X\right\rangle_{\mathbb{C}}=b_{i}(i \in[m])\right\}, \tag{C}
\end{equation*}
$$

still admits a unique optimal solution, where $\langle X, Y\rangle_{\mathbb{C}}=$ $\operatorname{tr}\left(X^{\dagger} Y\right)$ and $\mathcal{H}_{+}^{n}$ denotes the set of $n \times n$ Hermitian positive semidefinite matrices.

Proof. First, we show that the study of a complex SDP can be reduced to an equivalent real SDP. This fact is well known but we provide a brief argument for completeness. Indeed, for any feasible solution $X=X_{\mathbb{R}}+i X_{\mathbb{C}} \in \mathcal{H}_{+}^{n}$, the constraint $\left\langle A_{i}, X\right\rangle_{\mathbb{C}}=b_{i}$ is equivalent to two constraints on its real and imaginary part, namely: $\left\langle A_{i}, X_{\mathbb{R}}\right\rangle=b_{i}$ and $\left\langle A_{i}, X_{\mathbb{C}}\right\rangle=0$. Furthermore, checking whether $X_{\mathbb{R}}+i X_{\mathbb{C}}$ is Hermitian PSD is equivalent to

$$
\left(\begin{array}{cc}
X_{\mathbb{R}} & -X_{\mathbb{C}}  \tag{E2}\\
X_{\mathbb{C}} & X_{\mathbb{R}}
\end{array}\right) \in \mathcal{S}_{+}^{n}
$$

Based on these observations we define the realification of
$\left(P_{\mathbb{C}}\right)$ as the following SDP over the real numbers:

$$
\begin{aligned}
\sup _{X, Y} & \langle C, X\rangle \\
\text { s.t. } & \left\langle A_{i}, X\right\rangle=b_{i}(i \in[m]) \\
& \left\langle A_{i}, Y\right\rangle=0(i \in[m]) \\
& \left(\begin{array}{cc}
X & -Y \\
Y & X
\end{array}\right) \in \mathcal{S}_{+}^{2 n} .
\end{aligned}
$$

Clearly, the solutions of $\left(P_{\mathbb{C}}\right)$ are in bijection with the solutions of the realification, and thus, to show that $\left(P_{\mathbb{C}}\right)$ has a unique solution it suffices to show that $\left(P_{\mathbb{R}}\right)$ has a unique solution. Bringing $\left(P_{\mathbb{R}}\right)$ into standard SDP form we arrive at the formulation:

$$
\begin{aligned}
\sup _{W} & \left(\begin{array}{cc}
C / 2 & 0 \\
0 & C / 2
\end{array}\right) \bullet W \\
\text { s.t. } & \left(\begin{array}{cc}
A_{i} / 2 & 0 \\
0 & A_{i} / 2
\end{array}\right) \bullet W=b_{i}(i \in[m]) \\
& \left(\begin{array}{cc}
0 & A_{i} / 2 \\
A_{i} / 2 & 0
\end{array}\right) \bullet W=0(i \in[m]) \\
X=Z, & Y+Y^{T}=0 \\
& W=\left(\begin{array}{cc}
X & Y \\
Y^{T} & Z
\end{array}\right) \in \mathcal{S}_{+}^{2 n}
\end{aligned}
$$

whose dual is to minimize the function $\sum_{i=1}^{m} \lambda_{i} b_{i}$ over all $\lambda_{i}, \mu_{j}, t_{i j}, z_{i j}$ satisfying
$\sum_{i=1}^{m} \lambda_{i}\left(\begin{array}{cc}A_{i} / 2 & 0 \\ 0 & A_{i} / 2\end{array}\right)+\sum_{i=1}^{m} \mu_{i}\left(\begin{array}{cc}0 & A_{i} / 2 \\ A_{i} / 2 & 0\end{array}\right)+$
$M Z^{*}=\left\langle M, A_{i}\right\rangle=0 \forall i \Longrightarrow M=0$.
$\sum_{i j=1}^{n} t_{i j}\left(\begin{array}{cc}E_{i j} & 0 \\ 0 & -E_{i j}\end{array}\right)+\sum_{i j=1}^{n} z_{i j}\left(\begin{array}{cc}0 & E_{i j} \\ E_{i j}^{T} & 0\end{array}\right)-\left(\begin{array}{cc}C / 2 & 0 \\ 0 & C / 2\end{array}\right) \succeq$ Putting everything together, we get $M_{1}=M_{2}=M_{3}=0$.
$\square$
[1] S. Popescu and D. Rohrlich, Phys. Lett. A 166, 293 (1992)
[2] D. Mayers and A. Yao, Quantum Info. Comput. 4, 273 (2004)
[3] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A 45, 455304 (2012).
[4] M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Vol. 4051 (Springer, 2006).
[5] B. S. Tsirel'son, J. Soviet Math. 36, 557 (1987).
[6] S. J. Summers and R. Werner, J. Math. Phys. 28, 2440 (1987).
[7] J. S. Bell, Physics (Long Island City, N.Y.) 1, 195 (1964)
[8] J. Kaniewski, Phys. Rev. Lett. 117, 070402 (2016)
(E4)
We conclude the proof by showing that $\left(\begin{array}{cc}Y^{*} & 0 \\ 0 & Y^{*}\end{array}\right)$ is a dual nondegenerate optimal solution for the realification. First, by dual feasibility we have $Y^{*}=\sum_{i=1}^{m} y_{i}^{*} A_{i}-C$ for appropriate scalars $y_{i}^{*}$. Setting $\lambda_{i}=y_{i}^{*}$ and all other dual variables to zero, we have established feasibility. Second, to show optimality note that $\left(\begin{array}{cc}X^{*} & 0 \\ 0 & 0\end{array}\right)$ is optimal for the realification, and furthermore, $\left(\begin{array}{cc}X^{*} & 0 \\ 0 & 0\end{array}\right) \bullet\left(\begin{array}{cc}Y^{*} & 0 \\ 0 & Y^{*}\end{array}\right)=0$. Lastly, to check nondegeneracy consider a symmetric matrix $M=\left(\begin{array}{ll}M_{1} & M_{2} \\ M_{2}^{T} & M_{3}\end{array}\right)$ satisfying

$$
0=\left(\begin{array}{ll}
M_{1} & M_{2}  \tag{E5}\\
M_{2}^{T} & M_{3}
\end{array}\right)\left(\begin{array}{cc}
Y^{*} & 0 \\
0 & Y^{*}
\end{array}\right)
$$

and

$$
\begin{gather*}
0=M \bullet\left(\begin{array}{cc}
A_{i} / 2 & 0 \\
0 & A_{i} / 2
\end{array}\right)=M \bullet\left(\begin{array}{cc}
0 & A_{i} / 2 \\
A_{i} / 2 & 0
\end{array}\right)=  \tag{E6}\\
=M \bullet\left(\begin{array}{cc}
E_{i j} & 0 \\
0 & -E_{i j}
\end{array}\right)=M \bullet\left(\begin{array}{cc}
0 & E_{i j} \\
E_{i j}^{T} & 0
\end{array}\right)  \tag{E3}\\
M_{1} Y^{*}=M_{2} Y^{*}=M_{3} Y^{*}=0 \tag{E7}
\end{gather*}
$$

Furthermore, using (E6), from the third equation we get $M_{1}=M_{3}$, from the first one we get $\left\langle M_{1}, A_{i}\right\rangle=0$, and from the second one $\left\langle M_{2}, A_{i}\right\rangle=0$. Summarizing, for all $k=1,2,3$ we have that

$$
M_{k} Z^{*}=0 \text { and }\left\langle M_{k}, A_{i}\right\rangle=0(i \in[m])
$$

As $Z^{*}$ is dual nondegenerate, it has the property that, for any $M \in \mathcal{S}^{n}$,

$$
M Z^{*}=\left\langle M, A_{i}\right\rangle=0 \forall i \Longrightarrow M=0
$$

[9] A. Tavakoli, M. Farkas, D. Rosset, J.-D. Bancal, and J. Kaniewski, arXiv preprint arXiv:1912.03225 (2019).
[10] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L.-C. Kwek, Phys. Rev. Lett. 122, 250403 (2019).
[11] S. Kochen and E. P. Specker, J. Math. Mech. 17, 59 (1967).
[12] T. Metger and T. Vidick, arXiv e-prints , arXiv:2001.09161 (2020), arXiv:2001.09161 |quantph]
[13] A. Cabello, S. Severini, and A. Winter, Phys. Rev. Lett. 112, 040401 (2014).
[14] A. Cabello, V. D'Ambrosio, E. Nagali, and F. Sciarrino, Phys. Rev. A 84, 030302 (2011)
[15] S. Mansfield and E. Kashefi, Physical review letters 121, 230401 (2018).
[16] D. Saha, P. Horodecki, and M. Pawłowski, New Journal of Physics 21, 093057 (2019).
[17] N. Delfosse, P. A. Guerin, J. Bian, and R. Raussendorf, Physical Review X 5, 021003 (2015).
[18] J. Singh, K. Bharti, et al., Physical Review A 95, 062333 (2017).
[19] H. Pashayan, J. J. Wallman, and S. D. Bartlett, Physical review letters 115, 070501 (2015).
[20] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Nature 510, 351 EP (2014)
[21] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969)
[22] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky, Phys. Rev. Lett. 101, 020403 (2008)
[23] G. Chiribella and X. Yuan, arXiv:1404.3348 (2014)
[24] G. Chiribella and X. Yuan, Inf. Comput. 250, 15 (2016).
[25] M. Malinowski, C. Zhang, F. Leupold, A. Cabello, J. Alonso, and J. Home, Physical Review A 98, 050102 (2018).
[26] F. M. Leupold, M. Malinowski, C. Zhang, V. Negnevitsky, A. Cabello, J. Alonso, and J. P. Home, Phys. Rev. Lett. 120, 180401 (2018)
[27] F. Pokorny, C. Zhang, G. Higgins, A. Cabello, M. Kleinmann, and M. Hennrich, Phys. Rev. Lett. 124, 080401 (2020)
[28] M. Kleinmann, O. Guehne, J. R. Portillo, J.-Å. Larsson,
and A. Cabello, New Journal of Physics 13, 113011 (2011).
[29] G. Fagundes and M. Kleinmann, Journal of Physics A: Mathematical and Theoretical 50, 325302 (2017).
[30] A. Cabello, M. Gu, O. Gühne, and Z.-P. Xu, Physical review letters 120, 130401 (2018).
[31] C. Budroni, Philosophical Transactions of the Royal Society A 377, 20190141 (2019).
[32] A. Cabello, M. Gu, O. Gühne, J.-Å. Larsson, and K. Wiesner, Physical Review A 94, 052127 (2016).
[33] A. Cabello, L. E. Danielsen, A. J. López-Tarrida, and J. R. Portillo, Physical Review A 88, 032104 (2013).
[34] M. Chudnovsky, N. Robertson, P. Seymour, and R. Thomas, Annals of mathematics, 51 (2006).
[35] K. Bharti, A. S. Arora, L. C. Kwek, and J. Roland, arXiv preprint arXiv:1811.05294 (2018).
[36] F. Alizadeh, J.-P. A. Haeberly, and M. L. Overton, Math. Program. 77, 111 (1997).
[37] L. P. Thinh, A. Varvitsiotis, and Y. Cai, arXiv preprint arXiv:1809.10886 (2018).
[38] A. Mantri, T. F. Demarie, N. C. Menicucci, and J. F. Fitzsimons, Phys. Rev. X 7, 031004 (2017)
[39] U. Feige, Combinatorica 17, 79 (1997).
[40] D. E. Knuth, The Electronic Journal of Combinatorics 1, 1 (1994).
[41] L. Lovász, IEEE Trans. Inf. Theory 25, 1 (1979).


[^0]:    * equal contribution

