

ARTICLE OPEN



An elegant scheme of self-testing for multipartite Bell inequalities

Ekta Panwar^{1,2}✉, Palash Pandya¹ and Marcin Wieśniak^{1,2}

Self-testing is the most accurate form of certification of quantum devices. While self-testing in bipartite Bell scenarios has been thoroughly studied, self-testing in the more complex multipartite Bell scenarios remains largely unexplored. We present a simple and broadly applicable self-testing scheme for N -partite correlation Bell inequalities with two binary outcome observables per party. To showcase the versatility of our proof technique, we obtain self-testing statements for the MABK and WWWŻB family of linear Bell inequalities and Uffink's family of quadratic Bell inequalities. In particular, we show that the N -partite MABK and Uffink's quadratic Bell inequalities self-test the GHZ state and anti-commuting observables for each party. While the former uniquely specifies the state, the latter allows for an arbitrary relative phase. To demonstrate the operational relevance of the relative phase, we introduce Uffink's complex-valued N partite Bell expression, whose extremal values self-test the GHZ states and uniquely specify the relative phase.

npj Quantum Information (2023)9:71 ; <https://doi.org/10.1038/s41534-023-00735-3>

INTRODUCTION

One of the most striking features of quantum theory is the deviation of its predictions for Bell experiments from the predictions of classical theories with local casual (hidden variable) explanations¹. This phenomenon is captured by quantum violation of statistical inequalities, which are satisfied by all local realistic theories, referred to as Bell inequalities². Experimental demonstrations of the loophole-free violation of such inequalities (e.g., refs. 3–5) imply the possibility of sharing intrinsically random private numbers among an arbitrary number of spatially separated parties which power unconditionally secure private key distribution schemes (for more information on Device-independent quantum cryptography see refs. 6–10). Such applications of Bell non-locality follow from the fact that the extent of Bell inequality violation can uniquely identify the specific entangled quantum states and measurements, a phenomenon referred to as *self-testing* (see refs. 11,12 for initial contributions and the recent review of the progress till now see ref. 13).

Self-testing statements are the most accurate form of certifications for quantum systems. Self-testing schemes allow us to infer the underlying physics of a quantum experiment, i.e., the state and the measurements (up to local isometry), without any characterization of the internal workings of the measurement devices, and based only on the observed statistics, i.e., treating the measurement devices as black boxes with classical inputs and outputs. Self-testing has found many applications in several areas like *device-independent randomness generation*^{8,14}, *quantum cryptography*⁹, *entanglement detection*¹⁵, *delegated quantum computing*^{16,17}. While self-testing in the bipartite Bell scenarios has been thoroughly studied, self-testing in more complex multipartite Bell scenarios (see Fig. 1) remains largely unexplored.

In a multipartite setting, self-testing has been demonstrated for graph states using stabilizer operators¹⁸. Self-testing of multipartite graph states and partially entangled Greenberger-Horne-Zeilinger (GHZ)¹⁹ states has been demonstrated using a stabilizer-based approach, and Bell inequalities explicitly constructed for the

state²⁰. In general, multipartite Bell inequalities explicitly tailored for self-testing of a multipartite entangled state can be obtained using convex optimization techniques such as linear programming and semi-definite programming (SDP)^{17,21–23}. However, the Bell inequalities obtained in this way are just suitable candidates for the self-testing of the given multipartite states, and the potential self-testing statements must be verified using numerical techniques (such as the Swap method), which tend to be computationally expensive for multipartite scenarios with more than four parties. Completely analytical self-testing statements have also been obtained for multipartite states such as the W and the Dicke states by reprocessing self-testing protocols of bipartite states^{24–26}. Furthermore, parallel self-testing statements for multipartite states can be obtained using categorical quantum mechanics²⁷. Finally, the Mayers-Yao criterion can also be utilized for self-testing of graph states when the underlying graph is a triangular lattice²⁸.

In this article, we prove self-testing statements for multipartite Bell scenarios without relying on the Bell-operator dependent sum-of-squares decomposition²⁹. Consequently, our methodology immediately extends to all multipartite Bell scenarios, where each spatially separated party has two observables with binary outcomes ± 1 . To exemplify our proof technique, we obtain self-testing statements for N party Mermin-Ardehali-Belinskii-Klyshko (MABK)^{30,31} and Werner-Wolf-Weinfurter-Żukowski-Brukner (WWWŻB)^{32–34} family of linear Bell inequalities. Moreover, our methodology enables the recovery of self-testing statements for Bell functions which are not only the mean value of a Hermitian operator. Specifically, to showcase the versatility of our methodology, we obtain self-testing statements for the maximal violation of N party Uffink's quadratic Bell inequalities, which form tight witnesses of genuine multipartite non-locality, and the novel Uffink's complex-valued N partite Bell expressions³⁵.

The paper is organized as follows. First, in the Results section we recall the formal definition of self-testing. Then, we present the requisite preliminaries and specify the families of multipartite Bell

¹Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, ul. Wita Stwosza 57, 80-308 Gdańsk, Poland.

²International Centre for Theory of Quantum Technologies, University of Gdańsk, ul. Wita Stwosza 63, 80-308 Gdańsk, Poland. ✉email: ekta.panwar@phdstud.ug.edu.pl

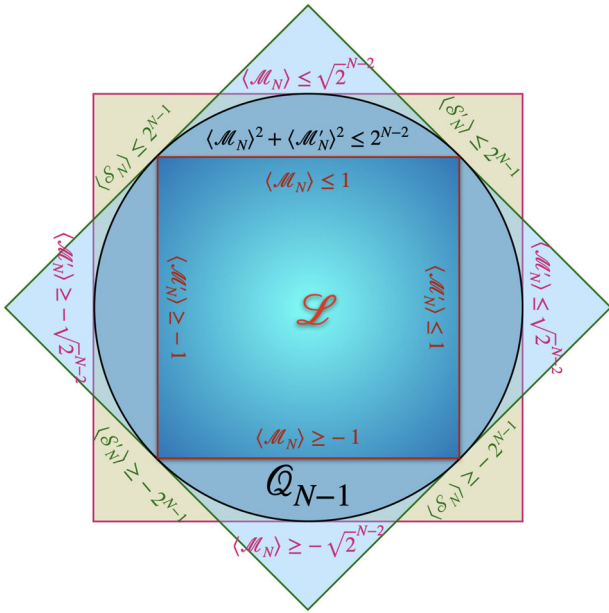


Fig. 1 Schematic representation of the correlations in multipartite Bell scenarios. This graphic is a schematic representation of the correlations in multipartite (involving arbitrary number N of spatially separated parties) Bell scenarios. Just like the bipartite Bell scenarios, the correlations which admit local hidden variable explanations form a convex polytope \mathcal{L} (shiny blue small horizontal square), whose facets are the N -party MABK inequalities [Eq. (2)] (red edges). However, the convex set of biseparable quantum correlations \mathcal{Q}_{N-1} (sky blue disk) does not form a polytope. Consequently, the linear inequalities such as the MABK [Eq. (2)] (pink edges of the large horizontal square) and Svetlichny inequalities [Eq. (3)] (green edges of the tilted square) do not form tight witnesses of genuine multipartite quantum non-locality. As the boundary of biseparable quantum correlations (black circle) is non-linear, Uffink's quadratic inequalities [Eq. (4)] form tighter witnesses of genuine multipartite quantum non-locality.

inequalities we consider in this article. Next, we develop the mathematical preliminaries of the self-testing scheme. In particular, we show that the observables of each party in two-setting binary outcome multipartite Bell scenarios can always be simultaneously represented as anti-diagonal matrices. Next, we utilize this anti-diagonal matrix representation to obtain self-testing statements for the maximal violations of N party MABK and tripartite WWWZB family of linear (on correlators) Bell inequalities. While the former serves to benchmark our scheme, the latter demonstrates the spectrum of situations one can encounter. Finally, we obtain self-testing statements for the maximal violation of N party Uffink's quadratic Bell inequalities and, at the very end of the Results section, we present the self-testing statements for the N partite Uffink's complex-valued Bell expressions. Next, we provide a brief discussion about the robustness of the self-testing statements obtained in this work. Finally, we conclude by providing a brief summary of our work and potential application.

RESULTS

Before presenting our results, let us first introduce the requisite preliminaries.

Self-testing in Bell scenarios

A Bell scenario describes the operational setup of a Bell experiment by specifying the following three components: (1) the number of spatially separated parties, (2) the number of inputs of each party specifying their measurement settings, (3) the

number of outcomes corresponding to each input per party specifying the measurement outcomes for each measurement setting for each party. Each party performs measurements on a quantum system they share. As there are no assumptions on the internal working mechanism of the experimental devices, we may consider the devices to be mere black boxes, capable of receiving inputs (measurement settings) and generating outputs (measurement outcomes). The parties perform measurements based on their inputs and record the corresponding measurement outcomes, and estimate the conditional joint probability distributions governing their devices. Now, the question is, what can we deduce from these experimental statistics? Specifically, can we make statements describing the underlying physics, i.e., the quantum state and measurements? Such statements are broadly referred to as self-testing statements.

Formally, we say that a given Bell scenario entailing N parties, $\{A_j\}_{j=1}^N$, each measuring two observables, $A^{(j)}, A'^{(j)}$ and sharing a state $|\bar{\psi}\rangle$ self-tests, if the observation of the quantum maximal value B of a given Bell expression \mathcal{B} implies that the state $|\bar{\psi}\rangle$ used in the experiment can be transformed by local unitaries, $\bigotimes_j U_{A_j}$, to a reference state, $|\psi\rangle$, and a separable junk part, $|\Psi\rangle$, on which the observables act trivially, i.e,

$$\bigotimes_j U_{A_j} |\bar{\psi}\rangle = |\psi\rangle \otimes |\Psi\rangle.$$

Likewise, the local observables $\{A^{(j)}\}_{j=1}^N$ and $\{A'^{(j)}\}_{j=1}^N$, satisfy,

$$U_{A_j} A^{(j)} (U_{A_j})^\dagger = A^{(j)} \otimes \mathbb{1},$$

$$U_{A_j} A'^{(j)} (U_{A_j})^\dagger = A'^{(j)} \otimes \mathbb{1},$$

where the joint observables $\bigotimes_j O^{(j)}$ where $O^{(j)} \in \{A^{(j)}, A'^{(j)}\}$ act on the Hilbert space of $|\psi\rangle, j$ and the tuple $\{|\psi\rangle, \{A^{(j)}, A'^{(j)}\}_j\}$ maximizes the given Bell expression, i.e., $\mathcal{B}(\{|\psi\rangle, \{A^{(j)}, A'^{(j)}\}_j\}) = B$.

The original idea of self-testing was presented in ref. ¹¹ by Mayers and Yao. Over the last few years, a great deal of work has been done in this area, primarily focused on bipartite Bell scenarios. However, self-testing in multipartite Bell scenarios remains relatively unexplored. In this paper, we obtain self-testing statements for multipartite Bell inequalities, introduced in the next section.

Two-setting N-party correlation Bell inequalities

This section presents the requisite preliminaries and specifies the families of Bell inequalities considered in this article. Specifically, here we consider multipartite Bell scenarios entailing N spatially separated (hence non-signaling) parties. We restrict ourselves to Bell scenarios where each party A_j , where $j \in \{1, \dots, N\}$, has two binary outcome observables $A^{(j)}, A'^{(j)}$ (Since there is no restriction on dimension, we can always take the measurements to be projective, in light of Naimark's dilation Theorem. The projectivity of measurements is a distinguishing feature of a broadly subscribed viewpoint on quantum theory, namely, "The Church of the larger Hilbert space"). In contrast to the well-studied bipartite Bell scenarios, multipartite scenarios are substantially richer in complexity. While the notion of multipartite locality is an obvious extension of bipartite locality, multipartite behaviors can be non-local in many distinct ways. Apart from this, the most significant impediment in obtaining self-testing statements for multipartite Bell scenarios is that they do not admit simplifying characterizations such as Schmidt decomposition of the shared entangled state, unlike the bipartite Bell scenarios.

Typically, Bell inequalities comprise a Bell expression and a corresponding local causal bound. The violation of Bell inequalities witnesses the non-locality of the underlying behaviors. In the rest of this section, we introduce the families of multipartite Bell

inequalities, for which we demonstrate self-testing statements using our proof technique.

Linear inequalities

The most frequently used Bell inequalities comprise Bell expressions which are linear expressions of observed probabilities. Our self-testing argument is immediately applicable for any Bell inequality whose Bell expression is the mean of any linear combination of N party operators of the form $\bigotimes_{j=1}^N O^{(j)}$, where $O^{(j)} \in \{A^{(j)}, A'^{(j)}\}$. Among such linear Bell inequalities, we consider the Werner-Wolf-Weinfurter-Żukowski-Brukner(WWWŻB) families of correlation Bell inequalities for which there exists a well-defined systematic characterization³⁶. The Bell operator for the WWWŻB family of Bell inequalities has the following general form,

$$\mathcal{W}_N = \frac{1}{2^N} \sum_{s_1, \dots, s_N = \pm 1} S(s_1, \dots, s_N) \bigotimes_{j=1}^N (A^{(j)} + s_j A'^{(j)}), \tag{1}$$

where $S(s_1, \dots, s_N)$ is an arbitrary function of the indices $s_1, \dots, s_N \in \{-1, 1\}$ with binary outcomes ± 1 . Every tight (WWWŻB) inequality is given by $\langle \mathcal{W}_N \rangle \leq_{\mathcal{L}} 1$, where $\langle O \rangle = \text{Tr}\{\rho O\}$ is the expectation value of the linear operator O with respect to the quantum state ρ , and $\leq_{\mathcal{L}}$ signifies that the inequality holds for all correlations which admit local hidden variable explanations (\mathcal{L})³⁷.

Next, we introduce a sub-family of (WWWŻB) Bell inequalities, the Mermin-Ardehali-Belinskii-Klyshko (MABK) family of inequalities, featuring one inequality for any number N of parties^{30,31,38}. Moreover, in the following subsection, we introduce non-linear (quadratic) Bell inequalities composed of these MABK inequalities. The N -party MABK operators can be obtained recursively as,

$$\begin{aligned} \mathcal{M}_N &= \frac{1}{2} (\mathcal{M}_{N-1} \otimes (A^{(j)} + A'^{(j)}) \\ &\quad + \mathcal{M}'_{N-1} \otimes (A^{(j)} - A'^{(j)})) \\ &= \frac{1}{2^{\frac{N+1}{2}}} \left(\left(\frac{1+i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \bigotimes_{j=1}^N (A^{(j)} + i A'^{(j)}) \right. \\ &\quad \left. + \left(\frac{1+i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \bigotimes_{j=1}^N (A^{(j)} - i A'^{(j)}) \right), \end{aligned} \tag{2}$$

where the complimentary MABK Bell expression \mathcal{M}'_{N-1} has the same form as \mathcal{M}_{N-1} but with all $A^{(j)}$ and $A'^{(j)}$ interchanged. The corresponding Bell inequalities are of the form, $\langle \mathcal{M}_N \rangle \leq_{\mathcal{L}} 1$. Whereas the maximum attainable values of $\langle \mathcal{M}_N \rangle$ for biseparable \mathcal{Q}_{N-1} , and generic quantum correlations \mathcal{Q} are $2^{\frac{N-2}{2}}$, and $2^{\frac{N-1}{2}}$, respectively. The maximal quantum value can be attained with anti-commuting local observables and the maximally entangled N -partite GHZ state³⁹⁻⁴¹.

Finally, we present yet another relevant sub-family of the (WWWŻB) inequalities, referred to as Svetlichny inequalities³⁵, which were explicitly conceived to witness genuine N -partite non-locality. Moreover, the quadratic Bell inequalities featured in the following subsection can also be composed of N -partite Svetlichny-Bell inequalities. The Svetlichny operator can be formed of MABK operators [Eq. (2)] in the following way,

$$\mathcal{S}_N^\pm = \begin{cases} 2^{k-1} \left((-1)^{\frac{k(k\pm 1)}{2}} \mathcal{M}_N^\pm, \right. \\ \text{(for } N = 2k); \\ 2^{k\pm 1} \left((-1)^{\frac{k(k\pm 1)}{2}} \mathcal{M}_N \mp (-1)^{\frac{k(k\mp 1)}{2}} \mathcal{M}_N \right), \\ \text{(for } N = 2k + 1), \end{cases} \tag{3}$$

where \mathcal{M}_N^+ is equivalent to \mathcal{M}_N [Eq. (2)] and \mathcal{M}_N^- is equivalent to \mathcal{M}'_N . The corresponding Svetlichny inequalities are of the form, $\langle \mathcal{S}_N^\pm \rangle \leq_{\mathcal{Q}_{N-1}} 2^{N-1} \leq_{\mathcal{Q}} 2^{N-\frac{1}{2}}$.

Quadratic inequalities

In bipartite Bell scenarios, without loss of generality, it is enough to consider linear Bell inequalities to witness non-locality as the set of behaviors that admit a local casual explanation form a convex polytope demarcated by linear facet inequalities. In contrast to the bipartite case, non-linear Bell inequalities form tighter witnesses of genuine multipartite non-locality. In multipartite Bell scenarios, the convex set of biseparable quantum behaviors does not form a polytope. Consequently, Uffink's quadratic Bell inequalities form stronger witnesses of genuine multipartite non-locality than the linear inequalities. There are two distinct families of N party quadratic Bell inequalities formed of the MABK [Eq. (2)] and Svetlichny [Eq. (3)], families of linear inequalities, \mathcal{U}_N^M and \mathcal{U}_N^S , respectively, which have the form

$$\mathcal{U}_N^M = \langle \mathcal{M}_N \rangle^2 + \langle \mathcal{M}'_N \rangle^2 \leq_{\mathcal{Q}_{N-1}} 2^{N-2} \leq_{\mathcal{Q}} 2^{N-1}, \tag{4}$$

$$\mathcal{U}_N^S = \langle \mathcal{S}_N^+ \rangle^2 + \langle \mathcal{S}_N^- \rangle^2 \leq_{\mathcal{Q}_{N-1}} 2^{2N-2} \leq_{\mathcal{Q}} 2^{2N-1}, \tag{5}$$

Characterizing local observables

In this section, we obtain a characterization for the binary outcome local observables $A = A^{(j)}$ and $A' = A'^{(j)}$ on an arbitrary Hilbert space $\mathcal{H} = \mathcal{H}^{(j)}$ for any given party \mathcal{A}_j , where $j \in \{1, \dots, N\}$. As in Bell scenarios, there is no restriction on the dimension of the underlying Hilbert space, using Naimark's dilation Theorem, without loss of generality, we can take the observables A and A' to be projective, i.e., $A^2 = A'^2 = \mathbb{1}$. First, via the following lemma, we demonstrate that the second observable A' can be split into two observables, one which commutes with the first observable A and one which anti-commutes with A ,

Lemma 1. Given any two binary outcome projective observables A and A' , A' can be decomposed as the sum of two observables $-\mathbb{1} \leq A'_\pm \leq \mathbb{1}$ and $-\mathbb{1} \leq A'_\pm \leq \mathbb{1}$, such that $[A, A'_+] = 0$, $\{A, A'_-\} = 0$, $\{A'_+, A'_-\} = 0$ and $(A'_\pm)^2 + (A'_\mp)^2 = \mathbb{1}$.

Proof. Without loss of generality, the binary outcome projective observable A can be represented as a diagonal matrix with positive and negative eigenvalues grouped together,

$$A = \begin{pmatrix} \mathbb{1}_m & 0 \\ 0 & -\mathbb{1}_n \end{pmatrix}, \tag{6}$$

where $\mathbb{1}_m$ is the $m \times m$ identity operator. With respect to A , the binary outcome projective observable A' has the following generic matrix representation,

$$A' = \begin{pmatrix} D_1 & D_2 \\ D_2^\dagger & D_3 \end{pmatrix}. \tag{7}$$

such that,

$$A'_- = \begin{pmatrix} 0 & D_2 \\ D_2^\dagger & 0 \end{pmatrix}, \tag{8}$$

$$A'_+ = \begin{pmatrix} D_1 & 0 \\ 0 & D_3 \end{pmatrix}. \tag{9}$$

Clearly, $[A, A'_+] = 0$, and $\{A, A'_-\} = 0$. As A' is projective we have,

$$\begin{aligned} (A')^2 &= (A'_+)^2 + (A'_-)^2 + \{A'_+, A'_-\} \\ &= \begin{pmatrix} D_1^2 + D_2 D_2^\dagger & D_1 D_2 + D_2 D_3 \\ D_2^\dagger D_1 + D_3 D_2^\dagger & D_2^\dagger D_2 + D_3^2 \end{pmatrix} \end{aligned} \tag{10}$$

$$= \mathbb{1}, \tag{11}$$

which requires the off-diagonal blocks to be zero,

$$\begin{aligned} \{A'_+, A'_-\} &= \begin{pmatrix} 0 & D_1 D_2 + D_2 D_3 \\ D_2^\dagger D_1 + D_3 D_2^\dagger & 0 \end{pmatrix} \\ &= 0, \end{aligned} \quad (12)$$

and leaves $(A'_+)^2 + (A'_-)^2 = \mathbb{1}$, which completes the proof.

Using the above Lemma, the relation between the eigenvalues of A' , A'_- , and A'_+ can be ascertained to be $\lambda_{A'}^i = \pm \sqrt{(\lambda_{A'_-}^i)^2 + (\lambda_{A'_+}^i)^2} = \pm 1$, where λ^i denotes the i^{th} eigenvalue⁴². So that the eigenvalues can be without loss of generality taken as $\pm \sin \theta_i$ and $\pm \cos \theta_i$ for A'_- and A'_+ respectively.

Next, we show that the spectra of any two anti-commuting observables must be symmetric, and each observable maps the positive eigenspaces to the negative eigenspaces of the other.

Lemma 2. Given any two binary outcome anti-commuting projective observables, A and A'_- , such that $A^2 = \mathbb{1}$, their spectra must be symmetric (i.e., if $|\psi_\lambda\rangle$ is an eigenvector corresponding to the eigenvalue λ , then there exists a unique eigenvector $|\psi_{-\lambda}\rangle$ corresponding to the eigenvalue $-\lambda$). Moreover, A'_- acts on an effective even-dimensional Hilbert space $\bigoplus_i E_{\pm\lambda_i}^{A'_-}$ decomposed into the direct sum of the even-dimensional eigenspaces $E_{\pm\lambda_i}^{A'_-} = E_{\lambda_i}^{A'_-} \oplus E_{-\lambda_i}^{A'_-}$. Where, $E_{\lambda_i}^{A'_-}$ and $E_{-\lambda_i}^{A'_-}$ are eigenspaces corresponding to the non-zero eigenvalues λ_i and $-\lambda_i$, respectively.

Proof. From the anti-commutation relation it follows that, $AA'_- = -A'_-A$. As A is unitary and Hermitian, we can take A to the other side to sandwich A'_- , which leaves us with,

$$AA'_-A = -A'_-. \quad (13)$$

Further, taking trace on both sides of Eq. (13) yields,

$$\text{Tr}\{A'_-\} = 0. \quad (14)$$

This implies that the observable A'_- has a symmetric spectra, i.e., for each eigenvector corresponding to a non-zero eigenvalue λ_i there exists an eigenvector corresponding to the eigenvalue $-\lambda_i$, along with the null space or the kernel $\ker(A'_-)$. Without loss of generality, we can ignore the kernel as it does not contribute to the violation of Bell inequalities. Hence, we are left with the subspace, $\bigoplus_i E_{\pm\lambda_i}^{A'_-}$, where $E_{\pm\lambda_i}^{A'_-} = E_{\lambda_i}^{A'_-} \oplus E_{-\lambda_i}^{A'_-}$ is an even-dimensional subspace corresponding to the non-zero eigenvalues $\pm\lambda_i$. The diagonalizability of A'_- (Hermitian) implies that we can decompose this subspace into the direct sum of these eigenspaces (and the kernel $\ker(A'_-)$), which further implies that the effective subspace of such operators can be truncated to an even-dimensional subspace. Finally, as on this truncated subspace, $AA'_-|\psi_{\lambda_i}\rangle = -\lambda_i A'_-|\psi_{\lambda_i}\rangle$, where $|\psi_{\lambda_i}\rangle$ is an eigenvector of A corresponding to eigenvalue $\lambda_i = \pm 1$, we conclude that $m = n$, i.e., A is even-dimensional and has a similarly symmetric spectrum.

Now, as $A' = A'_+ + A'_-$, the effective subspaces of A'_+ , A' , can also be truncated to the same effective even-dimensional subspace as A'_- . Also, as on this truncated subspace, $A'_+ A'_- |\psi_{\lambda_i}\rangle = -\lambda_i A'_- |\psi_{\lambda_i}\rangle$, where $|\psi_{\lambda_i}\rangle$ is an eigenvector of A'_+ corresponding to its eigenvalue λ_i , i.e., A'_+ has a similar symmetric spectrum. Moreover, Lemma 2 yields the following succinct parameterization of the two mutually anti-commuting components of any projective observable,

Corollary 2.1. Given two even-dimensional anti-commuting operators A_+ and A_- such that $(A'_+)^2 + (A'_-)^2 = \mathbb{1}$, they can be written in the form,

$$A'_{\pm|\theta_i} = \cos \theta_i B_{\pm|\theta_i}, \quad A'_{-|\theta_i} = \sin \theta_i B_{-|\theta_i}, \quad (15)$$

when restricted to the subspace $E_{+\theta_i}^{A'_+} \oplus E_{-\theta_i}^{A'_-}$ with corresponding eigenvalues $\pm \cos(\theta_i)$ for A_+ and $\pm \sin(\theta_i)$ for A_- , such that the operators $B_{\pm|\theta_i}$ are traceless and projective.

Proof. We have already shown the dimension of the combined eigenspaces $E_{\lambda_i}^{A'_+} \oplus E_{-\lambda_i}^{A'_-}$ is even. Then the two anti-commuting operators A'_+ and A'_- restricted to this eigenspace, denoted by $A'_{\pm|\theta_i}$ and $A'_{\mp|\theta_i}$, will only have eigenvalues $\pm \cos \theta_i$ and $\pm \sin \theta_i$ respectively, whilst still satisfying $(A'_{\pm|\theta_i})^2 + (A'_{\mp|\theta_i})^2 = \mathbb{1}$. It is then possible to write the same relation in terms of scaled operators, as

$$\cos^2 \theta_i B_{\pm|\theta_i}^2 + \sin^2 \theta_i B_{\mp|\theta_i}^2 = \mathbb{1}. \quad (16)$$

As a result, the operators $B_{\pm|\theta_i}$ have eigenvalues ± 1 that occur in pairs. Therefore, $\text{Tr}(B_{\pm|\theta_i}) = 0$ and $B_{\pm|\theta_i}^2 = \mathbb{1}$.

Using the above results, in such an even-dimensional subspace the following lemma holds.

Lemma 3. Given any two traceless and projective anti-commuting observables B_+ and B_- , the observable $\cos \alpha B_+ + \sin \alpha B_-$ is also traceless and projective.

Proof. Expanding the square,

$$\begin{aligned} &(\cos \alpha B_+ + \sin \alpha B_-)^2 \\ &= \cos^2 \alpha B_+^2 + \sin^2 \alpha B_-^2 + \cos \alpha \sin \alpha \{B_+, B_-\} \\ &= \mathbb{1}. \end{aligned} \quad (17)$$

And the trace is simply,

$$\cos \alpha \text{Tr}(B_+) + \sin \alpha \text{Tr}(B_-) = 0. \quad (18)$$

The above lemma shows that in the Bell scenarios considered here, the effective local dimension of any subsystem must be even-dimensional. Now, we present the main ingredient of our self-testing proof technique, i.e., the simultaneous anti-diagonal matrix representation for local observables of each party up to local isometries.

Theorem 4. Given any three binary outcome traceless and projective observables A , B_+ , and B_- , such that $[A, B_+] = 0$, $\{A, B_-\} = 0$, and $\{B_+, B_-\} = 0$, then these operators have a simultaneous anti-diagonal matrix representation.

Proof. As $[A, B_+] = 0$, we can take the dimension of the subspace for which the eigenvalues of A and B_+ are equal to be $2d_1$, and $2d_2$ for the subspace where the eigenvalues differ. Consequently, without loss of generality, by Lemma 2 the operators A , B_+ , and B_- have the following matrix representations,

$$\begin{aligned} A &= \begin{pmatrix} \mathbb{1}_{d_1} & & & \\ & \mathbb{1}_{d_2} & & \\ & & -\mathbb{1}_{d_2} & \\ & & & -\mathbb{1}_{d_1} \end{pmatrix}, \\ B_+ &= \begin{pmatrix} \mathbb{1}_{d_1} & & & \\ & -\mathbb{1}_{d_2} & & \\ & & \mathbb{1}_{d_2} & \\ & & & -\mathbb{1}_{d_1} \end{pmatrix}, \\ B_- &= \begin{pmatrix} & & & U_1 \\ & & U_2 & \\ & U_2^\dagger & & \\ U_1^\dagger & & & \end{pmatrix}. \end{aligned} \quad (19)$$

Since B_- is projective, U_1 and U_2 must be unitary. Thus, without altering A or B_+ we can take four unitaries V_1, V_2, V_3, V_4 , each acting on a different block, such that $V_1 U_1 V_4^\dagger = J_{d_1}$ and $V_2 U_2 V_3^\dagger = J_{d_2}$, where J_d is the row-reversed $d \times d$ identity matrix.

Consequently, we can now restrict ourselves to considering any one of the $d_1 + d_2$ two-dimensional subspaces, on which A and B_+ are represented by $\pm\sigma_z$, while B_- is projected onto σ_x . Finally, in each of these subspaces, we apply the following unitary transformation,

$$U = \frac{1}{2} \begin{pmatrix} -1 + i & 1 + i \\ -1 + i & -1 - i \end{pmatrix}, \quad (20)$$

which corresponds to a rotation by $\frac{2\pi}{3}$ with respect to axis $(1, 1, 1)$, and transforms $\sigma_z \rightarrow \sigma_x \rightarrow \sigma_y$, and bringing all three operators to strictly anti-diagonal form.

Summarizing, the Theorem 4, along with Lemmas 2 and 3 allow us to take the first observable of each party $A^{(j)}$ to be equivalent to σ_x on all relevant two-dimensional subspaces, while the second operator $A^{(j)}$ can be taken to be $A^{(j)} = \cos \theta_j \sigma_x + \sin \theta_j \sigma_y$.

We note here that the above thesis also follows from a well-known result, commonly referred to as Jordan's lemma^{43,44}, which states that any two dichotomic observables squaring to identity can be simultaneously brought into a block diagonal form with one and two-dimensional blocks. Discarding the one-dimensional blocks as they do not contribute to Bell non-locality, each pair of the remaining two-dimensional blocks, which act as dichotomic observables on the same Hilbert space can be unitarily rotated to σ_x and $\cos \theta_j \sigma_x + \sin \theta_j \sigma_y$. In fact, Jordan's lemma has already been used in this way to obtain self-testing statements⁴¹. Therefore, the contents of this section constitute an alternative proof of Jordan's lemma and the subsequent parametrization.

This theorem forms the key ingredient of our proof technique as it yields the following criterion for self-testing statements obtained in this work,

Lemma 5. The maximum quantum value B of any two-setting two outcome N -partite Bell expression \mathcal{B} composed of N party correlators, self-tests a generalized GHZ state, $\alpha \otimes_{j=1}^N |i_j\rangle + \beta \otimes_{j=1}^N |\bar{i}_j\rangle$, where $i_j \in \{0, 1\}$ and $\bar{i}_j = 1 \oplus i_j$, if the corresponding Bell operator has a non-degenerate maximum eigenvalue $\lambda_{max} = B$.

Proof. For two-setting binary outcome N partite Bell scenarios, Theorem 4 implies that the local observables of each party have simultaneous anti-diagonal matrix representations. Consequently, any N partite Bell expression \mathcal{B} composed only of N party correlators corresponds to a Bell operator on $(\mathbb{C}^2)^{\otimes N}$ which also has an anti-diagonal matrix representation. Clearly, the maximum value of the Bell expression \mathcal{B} corresponds to the maximum eigenvalue λ_{max} of the Bell operator. As the eigenvectors of any such anti-diagonal matrix are of the form of generalized GHZ states, $\alpha \otimes_{j=1}^N |i_j\rangle + \beta \otimes_{j=1}^N |\bar{i}_j\rangle$, where $i_j \in \{0, 1\}$ and $\bar{i}_j = 1 \oplus i_j$, the maximum value B of such a Bell expression self-tests such a state if the maximum eigenvalue λ_{max} of the Bell operator is non-degenerate.

In the next section, we demonstrate our proof technique and obtain self-testing statements for the MABK family of N party inequalities and tripartite Bell inequalities composed of three-party correlators.

Self-testing statements for multipartite inequalities

In this section, we use the tools developed in the previous section to obtain self-testing statements for linear MABK family of N party inequalities [Eq. (2)], and sketch the proofs for the self-testing statements for all distinct equivalence classes of tripartite WWWZB

facet inequalities [Eq. (1)]. Finally, we obtain self-testing statements for Uffink's family [Eq. (4)] of non-linear N party inequalities.

N party MABK inequalities

Theorem 6. In order to achieve maximal quantum violation of a N -party MABK inequality, $\langle \mathcal{M}_N \rangle = 2^{\frac{N-1}{2}}$, the parties must share a N qubit GHZ state $|\text{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$, where $\phi(N)$ is the relative phase, $\phi(N) = 0$ when N is odd, $\phi(N) = -\frac{\pi}{4}$ when N is even and perform maximally anti-commuting projective measurements $A^{(j)} = \sigma_x$ and $A^{(j)} = \sigma_y$ (up to local isometries).

Proof. From Lemma 2 and Theorem 4, without loss of generality, the local observables of any party \mathcal{A}_j , where $j \in \{1, \dots, N\}$, can be taken to be,

$$\begin{aligned} A^{(j)} &= \sigma_x, \\ A^{(j)} &= \cos \theta_j \sigma_x + \sin \theta_j \sigma_y, \end{aligned} \quad (21)$$

acting on the effective two-dimensional subspace. This parametrization implies that the MABK operator [Eq. (2)] \mathcal{M}_N has the following anti-diagonal matrix representation,

$$\mathcal{M}_N = \text{adiag} \begin{pmatrix} \frac{1}{2^{\frac{N-1}{2}}} \left(\left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{-i\theta_j}) \right) \\ + \left(\frac{1+i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 - ie^{-i\theta_j}) \\ \vdots \\ \frac{1}{2^{\frac{N-1}{2}}} \left(\left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{i\theta_j}) \right) \\ + \left(\frac{1+i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 - ie^{i\theta_j}) \end{pmatrix}, \quad (22)$$

where adiag represents a matrix with non-zero values only on the anti-diagonal. It is easy to see for any combination, $\forall j \in \{1, \dots, N\} : \theta_j = \pm \frac{\pi}{2}$, one of the anti-diagonal elements attains the maximum absolute value of $2^{\frac{N-1}{2}}$ while the others vanish.

Recall that the maximum expectation value of an operator corresponds to its highest eigenvalue, attained when the state corresponds to the associated eigenvector. Moreover, the eigenvectors of operators with an anti-diagonal matrix representation are of the generic form, $\alpha \otimes_{j=1}^N |i_j\rangle + \beta \otimes_{j=1}^N |\bar{i}_j\rangle$, where $i_j \in \{0, 1\}$ and $\bar{i}_j = 1 \oplus i_j$. Now, taking the expectation value of \mathcal{M}_N with respect to any one of these states selects the sum of a pair of (equidistant from the top and the bottom) anti-diagonal elements. As each such pair is equivalent to the rest up-to local rotations, we can, without loss of any generality, consider the state, $|\psi_N\rangle = \alpha|0\rangle^{\otimes N} + \beta|1\rangle^{\otimes N}$, which effectively yields a weighted sum of the top and bottom anti-diagonal elements of the matrix [Eq. (22)].

Specifically, the expectation value of the Hermitian operator \mathcal{M}_N for the state $|\psi_N\rangle$ has the expression,

$$\begin{aligned} \langle \psi_N | \mathcal{M}_N | \psi_N \rangle &= 2\text{Re} \left\{ \bar{\alpha} \frac{1}{2^{\frac{N-1}{2}}} \left(\left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{-i\theta_j}) \right) \right. \\ &\quad \left. + \left(\frac{1+i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 - ie^{-i\theta_j}) \right\} \beta, \end{aligned} \quad (23)$$

Using the fact that $\forall \alpha, \beta \in \mathbb{C} : \text{Re} \alpha \beta \leq |\alpha \beta| = |\alpha| |\beta|$ we bound $\langle \psi_N | \mathcal{M}_N | \psi_N \rangle$ from above in the following way,

$$\begin{aligned} \langle \psi_N | \mathcal{M}_N | \psi_N \rangle &\leq 2|\bar{\alpha}| |\beta| \frac{1}{2^{\frac{N-1}{2}}} \left(\left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{-i\theta_j}) \right) \\ &\quad + \left(\frac{1+i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 - ie^{-i\theta_j}) \Big|. \end{aligned} \quad (24)$$

As $|\alpha|^2 + |\beta|^2 = 1$, the maximum value of the above expression can only be attained for $|\alpha| = |\beta| = \frac{1}{\sqrt{2}}$, which picks out $|GHZ_N\rangle$ as the shared state. Consequently, we retrieve the following upper bound,

$$\langle \psi_N | \mathcal{M}_N | \psi_N \rangle \leq \left| \frac{1}{2^{\frac{N-1}{2}}} \left(\left(\frac{1+i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{-i\theta_j}) + \left(\frac{1+i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 - ie^{-i\theta_j}) \right) \right|. \quad (25)$$

Now, as $\left| \left(\frac{1+i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \right| = \left| \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \right| = 1$ and $|(1 + ie^{-i\theta_j})| = |2 \sin(\frac{\pi}{4} + \frac{\theta_j}{2})|$ and $|(1 - ie^{-i\theta_j})| = |2 \cos(\frac{\pi}{4} + \frac{\theta_j}{2})|$, we can further upper bound the above expression as,

$$\langle \psi_N | \mathcal{M}_N | \psi_N \rangle \leq 2^{\frac{N-1}{2}} \left(\prod_{j=1}^N \left| \sin\left(\frac{\pi}{4} + \frac{\theta_j}{2}\right) \right| + \prod_{j=1}^N \left| \cos\left(\frac{\pi}{4} + \frac{\theta_j}{2}\right) \right| \right).$$

As, $\forall j: |\sin(\frac{\pi}{4} + \frac{\theta_j}{2})| \leq 1, |\cos(\frac{\pi}{4} + \frac{\theta_j}{2})| \leq 1$, we can further upper bound the above expression by discarding all but three terms corresponding to any $i, j, k \in \{1, \dots, N\}$, such that,

$$\begin{aligned} \langle \psi_N | \mathcal{M}_N | \psi_N \rangle &\leq 2^{\frac{N-1}{2}} \left(\left| \sin\left(\frac{2\theta_i + \pi}{4}\right) \sin\left(\frac{2\theta_j + \pi}{4}\right) \sin\left(\frac{2\theta_k + \pi}{4}\right) \right| \right. \\ &\quad \left. + \left| \cos\left(\frac{2\theta_i + \pi}{4}\right) \cos\left(\frac{2\theta_j + \pi}{4}\right) \cos\left(\frac{2\theta_k + \pi}{4}\right) \right| \right) \\ &\leq 2^{\frac{N-1}{2}}, \end{aligned} \quad (26)$$

where the proof of the second inequality has been deferred to the Supplementary Note. In the Supplementary Note, we also show that this inequality can only be saturated when $\theta_i = \theta_j = \theta_k = \frac{\pi}{2}$. As the choice of $i, j, k \in \{1, \dots, N\}$ is completely arbitrary, the inequality can only be saturated when $\forall j \in \{1, \dots, N\}: \theta_j = \frac{\pi}{2}$, i.e., when for each party the local observables maximally anti-commute. As these settings maximize the value of \mathcal{M}_N only for a unique pair of equidistant anti-diagonal entries, the state must be $|GHZ_N\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$, where $\phi(N) = 0$ when N is odd, and $\phi(N) = -\frac{\pi}{4}$ when N is even, up to auxiliary degrees of freedom on which the measurements act trivially, and local basis transformations. This further implies that the actual shared state could be of the form $|GHZ_N\rangle \otimes |\Psi\rangle$ up to local unitaries, where the arbitrary state $|\Psi\rangle$ on auxiliary degrees of freedom does not contribute to the operational Bell violation and thus is referred to as the junk state.

We note here that the same proof technique extends to the complementary MABK inequalities, \mathcal{M}_{IN} , defined in ‘‘Results: Two-setting N-party correlation Bell inequalities’’, as well, to yield the corresponding self-testing statements, summarized in the following Corollary.

Corollary 6.1. In order to achieve the maximal quantum violation of a N -party complementary MABK inequality, $\langle \mathcal{M}_{IN} \rangle = 2^{\frac{N-1}{2}}$, the parties must share a N qubit GHZ state $|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$, where $\phi(N) = \frac{\pi}{2}$ when N is odd, $\phi(N) = \frac{\pi}{4}$ when N is even and perform maximally anti-commuting projective measurements $A^{(i)} = \sigma_x$ and $A^{(j)} = \sigma_y$ (up to local isometries).

The proof follows a relatively straightforward modification of the proof of Theorem 6. However, these self-testing statements will be used in the next section for obtaining self-testing of Uffink’s quadratic inequalities. Moreover, the proof technique readily applies to the Svetlichny family of N -party inequalities as they are composed of the N -party MABK inequalities. Furthermore, the proof technique enables self-testing of a much broader class of N -

party WWWZB inequalities. To demonstrate this, we sketch the proofs for self-testing of tripartite WWWZB inequalities [Eq. (1)].

Tripartite WWWZB inequalities

In the case of tripartite Bell scenarios where each party has two input and output respectively, we have a 26-dimensional local correlation polytope that has 64 vertices and 53,856 faces⁴⁵. These faces can be grouped into 46 equivalence classes of Bell inequalities listed in ref. ⁴⁶, and out of which, we consider the non-trivial facet inequalities, which are composed of only three-party correlators and can be grouped into the following four equivalence classes.

The first class is composed of correlation inequalities equivalent (up-to relabeling) to the *Mermin’s inequality* $\langle \mathcal{M}_3 \rangle \leq 1$,

$$\frac{1}{2} (\langle A^{(1)} A^{(2)} A^{(3)} \rangle + \langle A^{(1)} A^{(2)} A^{(3)} \rangle + \langle A^{(1)} A^{(2)} A^{(3)} \rangle - \langle A^{(1)} A^{(2)} A^{(3)} \rangle) \leq 1.$$

For these inequalities, the proof of Theorem 6 directly applies³⁷. As a consequence, we retrieve the tripartite GHZ state $|GHZ_3\rangle$ as well as maximally anti-commuting local observables as necessary ingredients for the maximal quantum violation 2.

The second equivalence class of tripartite inequalities is that of *unbalanced inequalities*, which can be found in the ref. ⁴⁷ as the seventh inequality in Table I, and also specified below,

$$\begin{aligned} &(3 \langle A^{(1)} A^{(2)} A^{(3)} \rangle + \langle A^{(1)} A^{(2)} A^{(3)} \rangle \\ &+ \langle A^{(1)} A^{(2)} A^{(3)} \rangle + \langle A^{(1)} A^{(2)} A^{(3)} \rangle \\ &- \langle A^{(1)} A^{(2)} A^{(3)} \rangle - \langle A^{(1)} A^{(2)} A^{(3)} \rangle \\ &- \langle A^{(1)} A^{(2)} A^{(3)} \rangle + \langle A^{(1)} A^{(2)} A^{(3)} \rangle) \leq 4. \end{aligned}$$

The corresponding operator has an anti-diagonal matrix representation with values of the form,

$$4 + (-1 + e^{ik_1\theta_1})(-1 + e^{ik_2\theta_2})(-1 + e^{ik_3\theta_3}), \quad (27)$$

where $(k_1, k_2, k_3 \in \{-1, 1\})$. Unlike the MABK class of inequalities the absolute values of these anti-diagonal terms are maximized when $\cos \theta_j = -\frac{1}{3}$. Thus, yet again, the tripartite GHZ state $|GHZ_3\rangle$ is distinguished, but non maximally anti-commuting local observables are required for maximal quantum violation, $\frac{20}{3}$, of these inequalities.

We will next discuss the equivalence class of the *extended CHSH inequalities* of the form given below, which is listed as the third inequality in Table I of the ref. ⁴⁶,

$$\frac{1}{2} (\langle A^{(1)} A^{(2)} A^{(3)} \rangle + \langle A^{(1)} A^{(2)} A^{(3)} \rangle + \langle A^{(1)} A^{(2)} A^{(3)} \rangle - \langle A^{(1)} A^{(2)} A^{(3)} \rangle) \leq 1.$$

For these inequalities, the operator in the anti-diagonal matrix representation has elements of the form,

$$\frac{1}{2} \left(1 + e^{ik_1\theta_1} + e^{i(k_2\theta_2 + k_3\theta_3)} - e^{i(k_1\theta_1 + k_2\theta_2 + k_3\theta_3)} \right). \quad (28)$$

Consequently, the corresponding absolute values are $2\sqrt{1 \pm \sin \theta_1 \sin(k_2\theta_2 \pm k_3\theta_3)}$. Clearly, for the maximal quantum violation, the operators $A^{(1)}$ and $A^{(1)}$ must maximally anti-commute, i.e., $\theta_1 = \pm \frac{\pi}{2}$. However, the maximal quantum violation only requires the sum $k_2\theta_2 \pm k_3\theta_3 = \pm \frac{\pi}{2}$, i.e., the optimal $A^{(2)}$ is defined only in reference to $A^{(3)}$. Clearly, for the maximal quantum violation $2\sqrt{2}$ the shared state must be equivalent to the bipartite maximally entangled state $|GHZ_2\rangle$. However, these inequalities do not satisfy the strict self-testing criterion as defined in section II, as the optimal local observables are not unique and specified only up-to a mutual relation.

Lastly, we have the equivalence class of the *CHSH-like inequalities* of the form given below, which correspond to the second

inequality listed in Table I of the ref. 47,

$$\frac{1}{2} (\langle A^{(1)} A^{(2)} A^{(3)} \rangle + \langle A^{(1)} A^{(2)} A^{(3)} \rangle + \langle A^{(1)} A^{(2)} A^{(3)} \rangle - \langle A^{(1)} A^{(2)} A^{(3)} \rangle) \leq 1.$$

These inequalities are equivalent to the CHSH or \mathcal{M}_2 inequality for which the proof of Theorem 6 directly applies. The non-zero elements of the anti-diagonal matrix representation of the corresponding Bell operator are of the form,

$$\left(1 + e^{ik_1\theta_1} + e^{ik_2\theta_2} - e^{i(k_1\theta_1+k_2\theta_2)} \right). \quad (29)$$

The modulo of these values is $2\sqrt{1 \pm \sin\theta_1 \sin\theta_2}$, which implies that for the maximum quantum violation $\sqrt{2}$ the observables for the first pair of parties must maximally anti-commute, i.e., $\pm\theta_1 = \pm\theta_2 = \frac{\pi}{2}$ and shared state must be equivalent to the bipartite maximally entangled state $|GHZ_2\rangle$.

Apart from the linear inequalities considered here, our proof technique, which relies on the anti-diagonal matrix representation of the Bell operator, is directly applicable to all two settings binary outcome linear (on correlators) multipartite Bell inequalities, either yielding perfect self-testing statements as defined in the beginning of the Results section, or pointing out the impossibility of them, as exemplified above. Next, we obtain self-testing statements using our proof technique for relevant classes of non-linear and complex-valued multipartite Bell expressions.

N party Uffink's quadratic Bell inequalities and complex Bell expression

As the convex set of biseparable multipartite quantum correlations does not form a polytope, linear inequalities like the Svetlichny inequalities [Eq. (3)] do not form tight, efficient witnesses of genuine multipartite non-locality. On the other hand, the non-linear inequalities such as the Uffink's family of $N \geq 3$ party quadratic (on correlators) inequalities [Eq. (4)] better capture the boundary of the quantum set of biseparable correlations and hence form better witnesses of genuine multipartite quantum non-locality. Here, we use our methodology to obtain self-testing statements for the maximum violation of Uffink's quadratic Bell inequalities. Specifically, we begin by linearizing Uffink's $N \geq 3$ party quadratic Bell expressions in the following way,

$$\langle \mathcal{U}_N^M \rangle = \langle \mathcal{M}_N \rangle^2 + \langle \mathcal{M}'_N \rangle^2 = |\langle \mathcal{M}_N \rangle \pm i \langle \mathcal{M}'_N \rangle|^2. \quad (30)$$

This follows from the simple observation that for any two real numbers $x_1, x_2 \in \mathbb{R}$, $x_1^2 + x_2^2 = |x_1 \pm ix_2|^2$, and the fact that the N -party MABK operator \mathcal{M}_N and the N -party complementary MABK operator \mathcal{M}'_N are Hermitian, such that $\langle \mathcal{M}_N \rangle, \langle \mathcal{M}'_N \rangle \in \mathbb{R}$. This linearization reduces our problem to considering a linear but non-Hermitian operator, $\tilde{\mathcal{U}}_N$, of the form,

$$\begin{aligned} \tilde{\mathcal{U}}_N &= (\mathcal{M}_N \pm i\mathcal{M}'_N) \\ &= \frac{1}{2^{N-1}} \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \bigotimes_{j=1}^N (A^{(j)} + iA^{(j)}), \end{aligned} \quad (31)$$

where the second equality is either satisfied by $\tilde{\mathcal{U}}_N = (\mathcal{M}_N + i\mathcal{M}'_N)$ or $\tilde{\mathcal{U}}_N = (\mathcal{M}_N - i\mathcal{M}'_N)$, depending on N , for instance, for $N \in \{2, 5, 6\}$ we have the former while for $N \in \{3, 4, 7\}$ we require the latter form of $\tilde{\mathcal{U}}_N$. With the linear operator in hand, we can now obtain the self-testing statement for \mathcal{U}_N^M , essentially by maximizing the modulo of the possibly complex expectation value of $\tilde{\mathcal{U}}_N$.

Theorem 7. In order to achieve maximal quantum violation of a N party Uffink's quadratic inequality, $\mathcal{U}_N^M = 2^{N-1}$, the parties must share a $N \geq 3$ qubit GHZ state $|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$, where $\phi(N) \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, and perform maximally anti-commuting projective measurements $A^{(j)} = \sigma_x$ and $A^{(j)} = \sigma_y$ (up to local isometries).

Proof. From Lemma 2 and Theorem 4, without loss of generality, the local observables of any party \mathcal{A}_j , where $j \in \{1, \dots, N\}$, can be taken to be,

$$\begin{aligned} A^{(j)} &= \sigma_x, \\ A^{(j)} &= \cos\theta_j\sigma_x + \sin\theta_j\sigma_y, \end{aligned} \quad (32)$$

acting on the effective two-dimensional subspace. This parametrization implies that Uffink's non-Hermitian operator [Eq. (31)], $\tilde{\mathcal{U}}_N$, has the following anti-diagonal matrix representation,

$$\tilde{\mathcal{U}}_N = \frac{1}{2^{\frac{N-1}{2}}} \text{adiag} \left(\begin{array}{c} \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{-i\theta_j}) \\ \vdots \\ \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{i\theta_j}) \end{array} \right), \quad (33)$$

where adiaj represents a matrix with non-zero values only on the anti-diagonal. It is easy to see for any combination, $\forall j \in \{1, \dots, N\} : \theta_j = \pm \frac{\pi}{2}$, one of the anti-diagonal element attains the maximum absolute value of $2^{\frac{N-1}{2}}$ while the others vanish.

Since, $\tilde{\mathcal{U}}_N$ has an anti-diagonal matrix representation, we know that the eigenvectors of such anti-diagonal matrices are of the generic form, $\alpha \bigotimes_{j=1}^N |i_j\rangle + \beta \bigotimes_{j=1}^N |\bar{i}_j\rangle$, where $i_j \in \{0, 1\}$ and $\bar{i}_j = 1 \oplus i_j$. Now, taking the expectation value of \mathcal{M}_N with respect to any one of these states selects the sum of a pair of (equidistant from the top and the bottom) anti-diagonal elements. As each such pair is equivalent to the rest up-to local rotations, we can, without loss of any generality, consider the state, $|\psi_N\rangle = \alpha|0\rangle^{\otimes N} + \beta|1\rangle^{\otimes N}$, which effectively yields a weighted sum of the top and bottom anti-diagonal elements of the matrix [Eq. (33)],

$$\begin{aligned} \mathcal{U}_N^M &= |\langle \psi_N | \tilde{\mathcal{U}}_N | \psi_N \rangle| \\ &= \frac{1}{2^{\frac{N-1}{2}}} \left| \left(\bar{\alpha} \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{-i\theta_j}) \beta \right. \right. \\ &\quad \left. \left. + \bar{\beta} \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{i\theta_j}) \alpha \right) \right| \\ &\leq \frac{1}{2^{\frac{N-1}{2}}} |\alpha| |\beta| \left(\left| \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{-i\theta_j}) \right| \right. \\ &\quad \left. + \left| \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{i\theta_j}) \right| \right), \end{aligned} \quad (34)$$

where for the inequality we employed the fact that $\forall \alpha, \beta \in \mathbb{C} : |\alpha + \beta| \leq |\alpha| + |\beta|$. Observe that, as $|\alpha|^2 + |\beta|^2 = 1$, the maximum value of the above expression can only be attained for $|\alpha| = |\beta| = \frac{1}{\sqrt{2}}$, which picks out $|GHZ_N\rangle$ as the shared state, $|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$. We note here that the relative phase $\phi(N) \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ is left completely unspecified, a fact that we explore thoroughly at the end of the proof in the following Corollary 7.1. Consequently, we retrieve the following upper bound,

$$\begin{aligned} |\langle \psi_N | \tilde{\mathcal{U}}_N | \psi_N \rangle| &\leq \frac{1}{2^{\frac{N-1}{2}}} \left(\left| \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{-i\theta_j}) \right| \right. \\ &\quad \left. + \left| \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \prod_{j=1}^N (1 + ie^{i\theta_j}) \right| \right). \end{aligned} \quad (35)$$

Now, as $\left| \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \right| = 1$ and $|(1 + ie^{-i\theta_j})| = |2 \sin(\frac{\pi}{4} + \frac{\theta_j}{2})|$ and $|(1 + ie^{i\theta_j})| = |2 \cos(\frac{\pi}{4} + \frac{\theta_j}{2})|$, we can further upper bound the above expression as,

$$\begin{aligned} |\langle \psi_N | \tilde{\mathcal{U}}_N | \psi_N \rangle| &\leq 2^{\frac{N-1}{2}} \left(\prod_{j=1}^N |\sin(\frac{\pi}{4} + \frac{\theta_j}{2})| \right. \\ &\quad \left. + \prod_{j=1}^N |\cos(\frac{\pi}{4} + \frac{\theta_j}{2})| \right). \end{aligned}$$

As, $\forall j : |\sin(\frac{\pi}{4} + \frac{\theta_j}{2})| \leq 1, |\cos(\frac{\pi}{4} + \frac{\theta_j}{2})| \leq 1$, we can further upper bound the above expression by discarding all but three terms

corresponding to $\forall i, j, k \in \{1, \dots, N\}$, such that,

$$\begin{aligned} & |\langle \psi_N | \tilde{\mathcal{U}}_N | \psi_N \rangle| \\ & \leq 2^{\frac{N-1}{2}} \left(\left| \sin\left(\frac{2\theta_i+\pi}{4}\right) \sin\left(\frac{2\theta_j+\pi}{4}\right) \sin\left(\frac{2\theta_k+\pi}{4}\right) \right| \right. \\ & \quad \left. + \left| \cos\left(\frac{2\theta_i+\pi}{4}\right) \cos\left(\frac{2\theta_j+\pi}{4}\right) \cos\left(\frac{2\theta_k+\pi}{4}\right) \right| \right) \\ & \leq 2^{\frac{N-1}{2}}, \end{aligned} \quad (36)$$

where the proof of the second inequality has been deferred to the Supplementary information. In the Supplementary information, we also show that this inequality can only be saturated when $\theta_i = \theta_j = \theta_k = \frac{\pi}{2}$, i.e., when for each party the local observables maximally anti-commute. Moreover, as these settings maximize a unique pair of equidistant anti-diagonal entries, while the others vanish, the state must be of the form, $|\text{GHZ}_N\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$, specified only up to the relative phase $\phi(N)$, up to auxiliary degrees of freedom on which the measurements act trivially, and local basis transformations. This further implies that the actual shared state could be of the form $|\text{GHZ}_N\rangle \otimes |\Psi\rangle$ with the arbitrary relative phase $\phi(N)$ of the GHZ state and the arbitrary state $|\Psi\rangle$ on auxiliary degrees of freedom which does not contribute to the operational Bell violation and thus is referred to as the junk state.

We would now like to highlight the difference between the self-testing statements for N partite linear MABK inequalities (Theorem 6 and Corollary 6.1) and Uffink's quadratic Bell inequalities (Theorem 7). Like the linear Bell inequalities, maximal violation of quadratic Bell inequalities fixes the local observables of each party to be maximally anti-commuting, such that without loss of generality they can be taken to be $A^{(i)} = \sigma_x$ and $A^{(j)} = \sigma_y$. However, while in the case of N partite linear MABK inequalities fixing the measurements exhausts all freedom up to local isometries and completely specifies the optimal state, on the other hand, the maximal violation of Uffink's quadratic inequalities does not uniquely specifies the optimal state. Specifically, the maximal violation of Uffink's quadratic inequalities can be attained with $|\text{GHZ}(\phi(N))\rangle$ where the relative phase $\phi(N)$ could take any value in $[-\frac{\pi}{2}, \frac{\pi}{2}]$. Hence, Uffink's quadratic inequalities do not strictly self-test. Below we show that strict self-testing statements can nevertheless be obtained for the complex-valued N partite Bell expression corresponding to the expectation value of Uffink's non-Hermitian operator $\langle \tilde{\mathcal{U}}_N \rangle$ [Eq. (31)] whenever the corresponding Uffink's quadratic Bell inequalities is maximally violated.

Until now, we have used our methodology to obtain self-testing statements for real valued linear and quadratic (on correlators) Bell expressions. We now discuss the case when our Bell expression takes complex values. Specifically, in the following Corollary, we obtain self-testing statements for the complex-valued Bell expression corresponding to the complex expectation value of $\langle \tilde{\mathcal{U}}_N \rangle$, where the operator $\tilde{\mathcal{U}}_N$ is defined in Eq. (31), using our methodology.

Corollary 7.1. In order to achieve extremal quantum value of the complex-valued Bell expression, $\langle \tilde{\mathcal{U}}_N \rangle = \langle \mathcal{M}_N \pm i \mathcal{M}'_N \rangle$, such that $|\langle \tilde{\mathcal{U}}_N \rangle| = 2^{\frac{N-1}{2}}$, the parties must share a $N \geq 3$ qubit GHZ state $|\text{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$, where $\phi(N) = \text{arccot}\left(\frac{\langle \mathcal{M}_N \rangle}{\langle \mathcal{M}'_N \rangle}\right)$ when N is odd, $\phi(N) = \text{arccot}\left(\frac{\langle \mathcal{M}_N \rangle}{\langle \mathcal{M}'_N \rangle}\right) - \frac{\pi}{4}$ when N is even and perform maximally anti-commuting projective measurements $A^{(i)} = \sigma_x$ and $A^{(j)} = \sigma_y$ (up to local isometries).

Proof. From Theorem 7, we know that the maximal quantum value of $\mathcal{U}_N^M = |\langle \tilde{\mathcal{U}}_N \rangle|^2 = 2^{N-1}$, self-tests the state to be maximally entangled N partite GHZ state, $|\text{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$,

where the relative phase $\phi(N)$ can be chosen arbitrarily. However, here we show that this relative phase $\phi(N)$ can still be operationally determined from the complex-valued Bell expression,

$$\langle \tilde{\mathcal{U}}_N \rangle = \langle \mathcal{M}_N \pm i \mathcal{M}'_N \rangle, \quad (37)$$

where $\langle \mathcal{M}_N \rangle$ and $\langle \mathcal{M}'_N \rangle$ are real valued complementary MABK Bell expressions for N parties, such that $|\langle \tilde{\mathcal{U}}_N \rangle|$ is $2^{\frac{N-1}{2}}$. We know that $|\langle \tilde{\mathcal{U}}_N \rangle| = 2^{\frac{N-1}{2}}$ implies that the local observables of each party can always be taken to be $A^{(i)} = \sigma_x$, $A^{(j)} = \sigma_y$, such that the operator $\tilde{\mathcal{U}}_N$ has the matrix representation [Eq. (33)]. Consequently,

$$\begin{aligned} \langle \tilde{\mathcal{U}}_N \rangle &= \langle \text{GHZ}_N | \tilde{\mathcal{U}}_N | \text{GHZ}_N \rangle \\ &= 2^{\frac{N-1}{2}} \left(\bar{\alpha} \left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} \beta \right) \end{aligned} \quad (38)$$

Up to experimentally indeterminable global phase, we can always take $\alpha = \frac{1}{\sqrt{2}}$ and $\beta = \frac{e^{i\phi}}{\sqrt{2}}$, such that Eq. (38) is simplified to,

$$\begin{aligned} \langle \tilde{\mathcal{U}}_N \rangle &= 2^{\frac{N-1}{2}} \left(\left(\frac{1-i}{\sqrt{2}} \right)^{(N-1) \bmod 2} e^{i\phi} \right) \\ &= \begin{cases} 2^{\frac{N-1}{2}} e^{i\phi}, & \text{iff } N \text{ is odd,} \\ 2^{\frac{N-1}{2}} e^{i(\phi - \frac{\pi}{4})}, & \text{else.} \end{cases} \end{aligned} \quad (39)$$

Next, with the aid of Eqs. (37) and (39), we can finally uniquely specify the relative phase $\phi(N)$ operationally. When $|\langle \tilde{\mathcal{U}}_N \rangle| = 2^{\frac{N-1}{2}}$ and the number of parties, N , is odd, the relative phase $\phi(N)$, must be precisely $\text{arccot}\left(\frac{\langle \mathcal{M}_N \rangle}{\langle \mathcal{M}'_N \rangle}\right)$, else $\phi(N) = \text{arccot}\left(\frac{\langle \mathcal{M}_N \rangle}{\langle \mathcal{M}'_N \rangle}\right) - \frac{\pi}{4}$ up to local isometries.

We note here that $\langle \tilde{\mathcal{U}}_N \rangle$, although complex, is an operational quantity, i.e., just like the value of linear Bell expressions, it can be directly estimated from the experimental statistics. Corollary 7.1 allows us to infer the relative phase $\phi(N)$ of the $N \geq 3$ qubit GHZ state from $\langle \tilde{\mathcal{U}}_N \rangle$. This fact is illustrated in Fig. 2.

Robust self-testing

The criterion for self-testing of a Bell inequality used in this work relies strongly on the assumption that the considered Bell expression attains its maximal value. However, in real experiments, this assumption cannot be fulfilled due to various experimental imperfections. Therefore, the self-testing statements must be made robust.

To make the self-testing statements obtained in this work robust, one can use the numerical SWAP method, which utilizes the Navascues-Pironio-Acin hierarchy to obtain bounds on the closeness (fidelity) of the experimental measurements and the shared state to the ideal self-testing measurements and state. Here we detail the technique for bounding the fidelity between the actual state and the reference self-testing state; the same can be applied to retrieve corresponding bounds for the measurements. The main idea of this technique relies on the notion of local isometries, which map the actual physical state $|\bar{\psi}\rangle$ to our reference self-testing state $|\psi\rangle$ and a junk state $|\Psi\rangle$ on local auxiliary systems. In most of the self-testing cases, these local isometries act as partial SWAP gates, essentially swapping the actual physical state $|\bar{\psi}\rangle$ with the state $|0\rangle^{\otimes N}$ of the registers, such that the final state of the registers corresponds to the reference self-testing state $|\psi\rangle$. It is often instructive to visualize the action of these local isometries as a SWAP circuit, which only depends on the self-testing measurements. The particulars of such a SWAP circuit, specifically those of the local isometries, enable us to express the fidelity, $\mathcal{F}_n = \langle \psi | \rho_{\text{SWAP}}(\Gamma_n) | \psi \rangle$, of the final state of the register $\rho_{\text{SWAP}}(\Gamma_n)$ with the target state $|\psi\rangle$, as a function of the entries of the necessarily positive semi-definite NPA moment matrix Γ_n of level $n \in \mathbb{N}$, as well as of the target self-testing state $|\psi\rangle$. As some of the entries of the moment matrix Γ_n correspond to

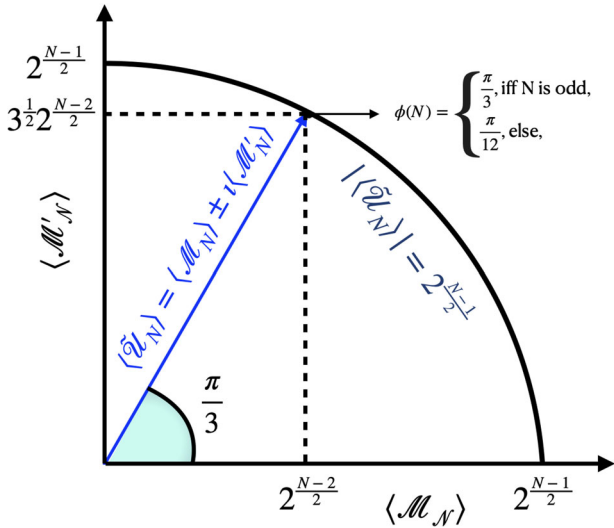


Fig. 2 Self-testing of the relative phase $\phi(N)$. This graphic schematically captures the self-testing statements for N partite Uffink’s quadratic Bell inequalities (Theorem 7), as well as the self-testing statements for the complex-valued Bell expressions corresponding to the mean value of Uffink’s non-Hermitian operator $\langle \tilde{\mathcal{U}}_N \rangle$ (Corollary 7.1). The figure depicts the complex plane on which the complex number $\langle \tilde{\mathcal{U}}_N \rangle = \langle \mathcal{M}_N \rangle \pm i \langle \mathcal{M}'_N \rangle$ lies, where $\langle \mathcal{M}_N \rangle$ is plotted on the real axis while $\langle \mathcal{M}'_N \rangle$ is plotted on the imaginary axis. The dark blue arc represents the boundary of the quantum set of correlations \mathcal{Q} characterized by the maximum violation of N partite Uffink’s quadratic Bell inequalities, $\mathcal{U}_N^M = |\langle \tilde{\mathcal{U}}_N \rangle|^2 = 2^{N-1}$. Crucially, for all points on the dark blue arc, Theorem 7 implies that the local observables of each party can be taken to be $A^{(j)} = \sigma_x$ and $A^{(j)} = \sigma_y$, and the state to be maximally entangled N partite GHZ state, $|\text{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$, where the relative phase $\phi(N)$ can be chosen arbitrarily (up to local isometries). However, using Corollary 7.1, even the relative phase can be uniquely identified by the observed value of $\langle \tilde{\mathcal{U}}_N \rangle$ if it lies on this arc. To exemplify this, we plot the specific case of $\langle \tilde{\mathcal{U}}_N \rangle = \langle \mathcal{M}_N \rangle \pm i \langle \mathcal{M}'_N \rangle = 2^{\frac{N-2}{2}} e^{i\frac{\pi}{3}}$ (light blue arrow), which uniquely specifies the relative phase to be $\phi(N) = \text{arccot}\left(\frac{\langle \mathcal{M}'_N \rangle}{\langle \mathcal{M}_N \rangle}\right) = \frac{\pi}{3}$ when N is odd, and $\phi(N) = \text{arccot}\left(\frac{\langle \mathcal{M}'_N \rangle}{\langle \mathcal{M}_N \rangle}\right) - \frac{\pi}{4} = \frac{\pi}{12}$ when N is even.

experimental statistics, such as $[\Gamma_n]_{\bar{A}^{(1)}\bar{A}^{(2)}} = \langle \bar{\psi} | \bar{A}^{(1)} \bar{A}^{(2)} | \bar{\psi} \rangle$, the behavioral preconditions of a self-testing statement translate to linear constraints on the entries of the moment matrix Γ_n . Given a target self-testing state $|\psi\rangle$ and solving the consequent semi-definite minimization program with the fidelity, $\mathcal{F}_n = \langle \psi | \rho_{\text{SWAP}}(\Gamma_n) | \psi \rangle$ as the linear objective function, retrieves a converging sequence of lower bounds, $\mathcal{F}_1 \leq \mathcal{F}_2 \dots \mathcal{F}_n$ such that $\mathcal{F}_{n \rightarrow \infty} = \mathcal{F}$, where \mathcal{F} is the quantum fidelity.

In Fig. 3, we depict the SWAP circuit corresponding to the N party self-testing statements obtained in this work for MABK inequalities (Theorem 6), complementary MABK inequalities (Corollary 6.1), Uffink’s quadratic inequalities (Theorem 7) and Uffink’s complex-valued Bell expressions (Corollary 7.1). As the self-testing measurements for all of these cases are the same, i.e., $A^{(j)} = \sigma_x$ and $A^{(j)} = \sigma_y$, the circuit in Fig. 3 effectively swaps the actual state $|\bar{\psi}_N\rangle$ (which attains the respective preconditions of these self-testing statements) with the state $|0\rangle^{\otimes N}$ of the registers, such that the final state of the registers corresponds to their respective self-testing maximally entangled N partite GHZ state, $|\text{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$. This, in turn, allows us to retrieve a converging sequence of lower bounds on the fidelity, $\mathcal{F}_n = \langle \text{GHZ}_N | \rho_{\text{SWAP}}(\Gamma_n) | \text{GHZ}_N \rangle$, in the aforementioned fashion.

As the resultant semi-definite programs, although straightforward to implement^{22,23}, are too computationally hard to solve efficiently without additional symmetry-based simplifications, we leave this as a future direction.

We now highlight the advantage of Uffink’s quadratic Bell inequalities and Uffink’s complex-valued Bell expressions over the linear MABK inequalities for robust self-testing in noisy experimental scenarios. Heuristically, as Uffink’s quadratic Bell inequalities and Uffink’s complex valued Bell expressions take two experimentally observable quantities into account, namely, the value of linear MABK inequality, $\langle \mathcal{M}_N \rangle$, as well as the value of linear complementary MABK inequality $\langle \mathcal{M}'_N \rangle$, they provide more accurate robust self-testing than when the latter are considered on their own.

Specifically, consider an experiment E aimed at robust self-testing of the N qubit GHZ state using N party MABK Bell expression, $\langle \mathcal{M}_N \rangle$. Suppose that the experiment yields the value $\langle \mathcal{M}_N \rangle_E = 2^{\frac{N-1}{2}} - \epsilon$, the fidelity \mathcal{F}_1 of the experimental state with the N qubit GHZ state optimal for $\langle \mathcal{M}_N \rangle$ (Theorem 6) is proportional to $2^{\frac{N-1}{2}} - \epsilon$. However, the experimental imperfections will inevitably yield experimental behavior for which $\langle \mathcal{M}'_N \rangle_E \neq 0$. Consequently, the experimental behavior will always be closer to the extremal point which attains $\langle \tilde{\mathcal{U}}_N \rangle =$

$\frac{2^{\frac{N-1}{2}}}{\sqrt{\langle \mathcal{U}'_N \rangle_E}} (\langle \mathcal{M}_N \rangle_E \pm i \langle \mathcal{M}'_N \rangle_E)$ as compared to the extremal point which attains $\langle \mathcal{M}_N \rangle = 2^{\frac{N-1}{2}}$ and $\langle \mathcal{M}'_N \rangle = 0$. Hence, the fidelity of the experimental state with the target GHZ state $|\text{GHZ}_N\rangle$ which realizes this extremal point (from Corollary 7.1) will yield a fidelity \mathcal{F}_2 proportional to $\sqrt{\langle \mathcal{U}'_N \rangle_E} = \sqrt{(2^{\frac{N-1}{2}} - \epsilon)^2 + \langle \mathcal{M}'_N \rangle_E^2}$, such that, $\mathcal{F}_2 > \mathcal{F}_1$. Hence, in general taking into account, Uffink’s quadratic and complex-valued Bell expressions provide for a more accurate and robust DI self-testing of the N qubit GHZ state as compared to the MABK inequalities, especially in cases when the relative phase is irrelevant to the application and could be arbitrary.

Consequently, Uffink’s quadratic and complex-valued Bell expressions provide for a more accurate and robust DI characterization of quantum systems in multipartite Bell scenarios as compared to the MABK inequalities.

DISCUSSIONS

Quantum correlations that violate Bell inequalities can certify the shared entangled state and local measurements in an entirely device-independent manner. This feature of quantum non-local correlations is referred to as self-testing. In this work, we presented a simple and broadly applicable proof technique to obtain self-testing statements for the maximum quantum violation of a large relevant class of multipartite (involving an arbitrary number N of spatially separated parties) Bell inequalities. Unlike the relatively straightforward bipartite Bell scenarios, the multipartite scenarios are substantially richer in complexity owing to the various types of multipartite non-locality.

The traditionally employed sum-of-squares-like proof techniques rely on the Bell inequality’s specific structure and the hermiticity of the corresponding Bell operator. Moreover, we recall here that finding the sum-of-squares decomposition for a linear Bell expression is the semi-definite programming dual of finding the maximum quantum value of the Bell expression, which in turn can be cast as an instance of the moment-based formulation Navascues-Pironio-Acin hierarchy of semi-definite programming relaxations^{48,49}. It follows from this semi-definite programming duality that the level of the moment-based Navascues-Pironio-Acin hierarchy required for saturation of the maximal quantum value of a Bell expression corresponds to the degree of the

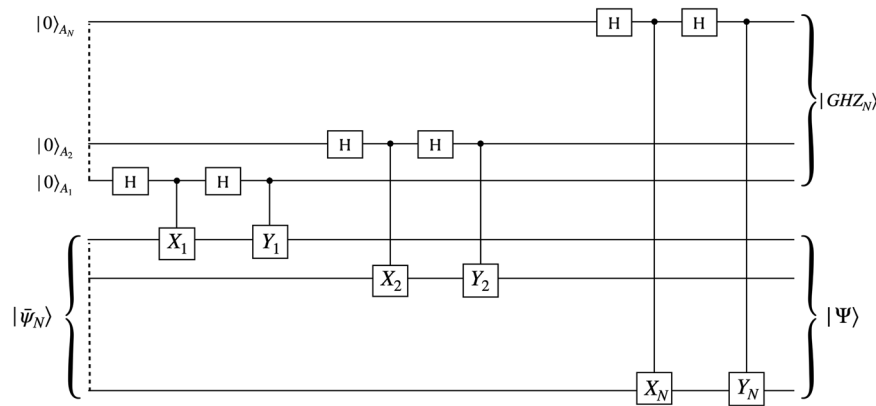


Fig. 3 Swap circuit. This graphic represents the partial SWAP gate isometry used to self-test maximally entangled N partite GHZ state $|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$. After the application of the circuit, the $|GHZ_N\rangle$ state is extracted from the actual experimental state $|\tilde{\psi}_N\rangle$ to the ancillary qubits. Here, H denotes a Hadamard gate, and $X_1, Y_1, X_2, Y_2, \dots, X_N, Y_N$ are the operators which act analogously to σ_x, σ_y on the actual state $|\tilde{\psi}_N\rangle$. As the circuit only depends on the self-testing measurements, this circuit works for the N partite self-testing statements obtained in this work, namely, the self-testing statements for MABK inequalities (Theorem 6), complimentary MABK inequalities (Corollary 6.1), Uffink's quadratic inequalities (Theorem 7) and Uffink's complex-valued Bell expressions (Corollary 7.1). As the self-testing measurements for all of these cases are the same, i.e., $A^{(i)} = \sigma_x$ and $A^{(j)} = \sigma_y$, the circuit SWAPs the actual state $|\tilde{\psi}_N\rangle$ (which attains the respective preconditions of these self-testing statements) with the state $|0\rangle^{\otimes N}$ of the registers, such that the final state of the registers corresponds to their respective self-testing maximally entangled N partite GHZ state.

polynomials in the sufficient sum-of-squares decomposition of the corresponding Bell operator. It is also easy to see that the minimum level $\lceil \frac{N}{2} \rceil$ of the moment-based Navascues-Pironio-Acin hierarchy degree required for the saturation of N party Bell inequalities, such as the MABK and the complimentary MABK family of Bell inequalities, increases with N , and so does the maximum degree of the polynomials in the corresponding sum-of-squares decomposition. Consequently, finding sum-of-squares decomposition becomes increasingly arduous for a large number N of spatially separated parties.

Although the Sum-of-Squares decomposition is applicable to any Bell scenario, more often than not, finding it can be challenging. In contrast, the technique presented in this paper offers a more state-forward approach. It is applicable to binary input and output Bell scenarios with an arbitrary number of spatially separated parties (N). It can derive self-testing statements for any Bell inequality in such Bell scenarios, as long as the associated Bell operator has an anti-diagonal matrix representation. In "Results: Characterizing local observables", we show that the observables of each party in two-setting binary outcome multipartite Bell scenarios can always be simultaneously represented as anti-diagonal matrices (Theorem 4). Consequently, in such scenarios, the Hermitian Bell operators corresponding to all Bell inequalities composed exclusively of N party correlators also have an anti-diagonal matrix representation. In "Results: Self-testing statements for multipartite inequalities", to demonstrate our proof technique, we obtain proofs of self-testing statements for the MABK family of N party inequalities (Theorem 6) (This constitutes a reproduction of the self-testing statements for MABK inequalities from ref. ³⁹, and hence serves as a preliminary certification of our proof technique.), followed by self-testing statements for the complimentary N party MABK inequalities (Corollary 6.1) and tripartite WWWZB inequalities ("Results: Tripartite WWWZB inequalities"). While the former self-testing statements demonstrate the relative simplicity and scalability (in the number of parties N) of our proof technique and serve as reliable benchmarks, the latter self-testing statements serve to exemplify all possible exceptions to perfect self-testing statements such as non-unique optimal states or observables, and non-anticommuting pairs of optimal measurements.

To further demonstrate the versatility of our proof technique which relies only on the anti-diagonal matrix representation of the

Bell operator and not even on its hermiticity, we obtain self-testing statements for Uffink's family of quadratic Bell inequalities (Theorem 7), as well as for the novel complex-valued Uffink's Bell expressions with corresponding non-Hermitian Bell operators (Corollary 7.1). As these quadratic and complex Bell expressions do not allow for sum-of-squares-like self-testing techniques, which rely on the linearity of the Bell expressions and on the hermiticity of the associated Bell operators, the self-testing statements obtained here form distinguishing applications of our proof technique.

One of the salient features of the multipartite self-testing statements obtained in this work, namely, for maximum quantum violation of MABK inequalities (Theorem 6), complimentary MABK inequalities (Corollary 6.1), Uffink's quadratic inequalities (Theorem 7) and extremal quantum values of Uffink's complex-valued Bell expressions (Corollary 7.1), is that they all uniquely single-out anti-commuting binary outcome observables for each party, which, without loss of generality, can be taken to be σ_x and σ_y , up to local isometries. On the other hand, these self-testing statements also pick out the maximally entangled N partite GHZ state $|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\phi(N)}|1\rangle^{\otimes N})$, where $\phi(N) \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ is the relative phase. However, while the self-testing statements for the MABK and the complimentary MABK inequalities uniquely specify $\phi(N)$, the self-testing statements for Uffink's quadratic Bell inequalities do not uniquely specify the phase $\phi(N)$. These observations lead to the self-testing statements (Corollary 7.1) for the extremal values of the novel Uffink's complex-valued Bell expressions, which effectively summarize the former statements. Specifically, fixing the local observables of each party to be σ_x and σ_y , Corollary 7.1 brings forth the one-to-one correspondence between the experimentally accessible extremal values of Uffink's complex-valued Bell expressions and the relative phase $\phi(N)$ of the N partite GHZ state, essentially demonstrating the operational relevance of the latter.

The N -party MABK inequalities [Eq. (2)] form efficient witnesses of genuine N -partite non-locality and entanglement and hence find applications in tasks that require the participation of all parties, i.e., the tasks in which no subset of the parties can succeed without the others⁴⁷, for example, quantum secret sharing⁵⁰, social welfare games⁵¹, DI randomness generation and expansion⁵², and conference key distribution schemes^{53,54}. The advantage of the MABK inequalities over the other inequalities in N -partite DI information processing and cryptography task springs

from its permutational symmetry, which does not privilege one party at the expense of the other parties. Uffink's quadratic inequalities [Eq. (4)] and complex-valued Bell expression [Eq. (31)] also retain this permutational symmetry while being strictly better at witnessing genuine N -partite non-locality and entanglement. The DI information processing and cryptographic applications are essentially fueled by the characterization of the quantum devices, enabled by the values of respective Bell expressions, as exemplified by the self-testing statements presented in this work. Consequently, as Uffink's quadratic inequalities and complex-valued Bell expression allow for a more accurate and robust certification of quantum devices, using them instead of MABK in DI applications can only benefit the respective performance.

Note added: During the preparation of the current work, we have become aware of ref. ⁵⁵. While it presents similar results, our proof technique, which constitutes the main conceptual contribution of this work, is substantially different from their proof technique. In particular, the key contrasting feature of our proof technique is its applicability to non-linear Bell inequalities.

DATA AVAILABILITY

Data accessibility is not applicable to this manuscript.

Received: 1 March 2022; Accepted: 21 June 2023;

Published online: 17 July 2023

REFERENCES

- Bell, J. S. On the Einstein Podolsky Rosen paradox. *Phys. Phys. Fiz.* **1**, 195–200 (1964).
- Brunner, N. et al. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).
- Hensen, B. et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015).
- Giustina, M. et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
- Shalm, L. K. et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
- Vazirani, U. & Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).
- Acín, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
- Colbeck, R. Quantum and relativistic protocols for secure multi-party computation Preprint at <https://doi.org/10.48550/arXiv.0911.3814> (2011).
- Ekert, A. & Renner, R. The ultimate physical limits of privacy. *Nature* **507**, 443–447 (2014).
- Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
- Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Inf. Comput.* **4**, 273–286 (2004).
- Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proc. 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, 503–509 (1998).
- Šupić, I. & Bowles, J. Self-testing of quantum systems: a review. *Quantum* **4**, 337 (2020).
- Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A Math. Theor.* **44**, 095305 (2011).
- Gheorghiu, A., Kapourniotis, T. & Kashefi, E. Verification of quantum computation: an overview of existing approaches. *Theory Comput. Syst.* **63**, 715–808 (2019).
- Bowles, J., Šupić, I., Cavalcanti, D. & Acín, A. Self-testing of Pauli observables for device-independent entanglement certification. *Phys. Rev. A* **98**, 042336 (2018).
- Sekatski, P., Bancal, J.-D., Wagner, S. & Sangouard, N. Certifying the building blocks of quantum computers from Bell's theorem. *Phys. Rev. Lett.* **121**, 180505 (2018).
- McKague, M. Self-testing graph states. *Theory of Quantum Computation, Communication, and Cryptography*, 104–120 (Springer, 2014).
- Greenberger, D. M., Zeilinger, A. & Horne, M. A. Going beyond Bell's theorem. *Bell's Theorem, Quantum Theory and Conceptions of the Universe* (ed Kafatos, M.) 73–76 (Kluwer Academic, 1989).
- Baccari, F., Augusiak, R., Šupić, I., Tura, J. & Acín, A. Scalable bell inequalities for qubit graph states and robust self-testing. *Phys. Rev. Lett.* **124**, 020402 (2020).
- Pál, K. F., Vértesi, T. & Navascués, M. Device-independent tomography of multipartite quantum states. *Phys. Rev. A* **90**, 042340 (2014).
- Bancal, J.-D., Navascués, M., Scarani, V., Vértesi, T. & Yang, T. H. Physical characterization of quantum devices from nonlocal correlations. *Phys. Rev. A* **91**, 022115 (2015).
- Yang, T. H., Vértesi, T., Bancal, J.-D., Scarani, V. & Navascués, M. Robust and versatile black-box certification of quantum devices. *Phys. Rev. Lett.* **113**, 040401 (2014).
- Wu, X. et al. Robust self-testing of the three-qubit W state. *Phys. Rev. A* **90**, 042339 (2014).
- Fadel, M. Self-testing Dicke states. Preprint at <https://doi.org/10.48550/arXiv.1707.01215> (2017).
- Šupić, I., Coladangelo, A., Augusiak, R. & Acín, A. Self-testing multipartite entangled states through projections onto two systems. *New J. Phys.* **20**, 083041 (2018).
- Buhrman, H. & Massar, S. Causality and Tsirelson's bounds. *Phys. Rev. A* **72**, 052103 (2005).
- Hayashi, M. & Hajdušek, M. Self-guaranteed measurement-based quantum computation. *Phys. Rev. A* **97**, 052308 (2018).
- Bamps, C. & Pironio, S. 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).
- Ardehali, M. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. *Phys. Rev. A* **46**, 5375–5378 (1992).
- Belinskii, A. V. & Klyshko, D. N. Interference of light and Bell's theorem. *Phys. Usp.* **36**, 653–693 (1993).
- Werner, R. F. & Wolf, M. M. All-multipartite Bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A* **64**, 032112 (2001).
- Weinfurter, H. & Żukowski, M. Four-photon entanglement from down-conversion. *Phys. Rev. A* **64**, 010102 (2001).
- Żukowski, M. & Brukner, I. C. V. Bell's theorem for general n -qubit states. *Phys. Rev. Lett.* **88**, 210401 (2002).
- Uffink, J. Quadratic bell inequalities as tests for multipartite entanglement. *Phys. Rev. Lett.* **88**, 230406 (2002).
- Scarani, V. The device-independent outlook on quantum physics. *Acta Phys.* **62**, 347 (2012).
- Żukowski, M. & Brukner, I. C. V. Bell's theorem for general n -qubit states. *Phys. Rev. Lett.* **88**, 210401 (2002).
- Mermin, N. D. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.* **65**, 1838 (1990).
- Kaniewski, J. M. K. Self-testing of binary observables based on commutation. *Phys. Rev. A* **95**, 062323 (2017).
- Pál, K. F., Vértesi, T. & Navascués, M. Device-independent tomography of multipartite quantum states. *Phys. Rev. A* **90**, 042340 (2014).
- Kaniewski, J. Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities. *Phys. Rev. Lett.* **117**, 070402 (2016).
- Ponomarenko, V. & Selstad, L. Eigenvalues of the sum and product of anti-commuting matrices. *J. Math.* **13**, 625–632 (2020).
- Pironio, S. et al. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021 (2009).
- Irfan, A. A. M., Mayer, K., Ortiz, G. & Knill, E. Certified quantum measurement of Majorana fermions. *Phys. Rev. A* **101**, 032106 (2020).
- Pitowsky, I. & Svozil, K. Optimal tests of quantum nonlocality. *Phys. Rev. A* **64**, 014102 (2001).
- Śliwa, C. Symmetries of the Bell correlation inequalities. *Phys. Rev. Lett.* **317**, 165–168 (2003).
- Sami, S., Chakrabarty, I. & Chaturvedi, A. Complementarity of genuine multipartite Bell nonlocality. *Phys. Rev. A* **96**, 022121 (2017).
- Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.* **10**, 073013 (2008).
- Ioannou, M. & Rosset, D. Noncommutative polynomial optimization under symmetry. Preprint at <https://doi.org/10.48550/arXiv.2112.10803> (2021).
- Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829–1834 (1999).
- Banik, M. et al. Two-qubit pure entanglement as optimal social welfare resource in Bayesian game. *Quantum* **3**, 185 (2019).
- Grasselli, F., Murta, G., Kampermann, H. & Bruß, D. Entropy bounds for multiparty device-independent cryptography. *PRX Quantum* **2**, 010308 (2021).
- Murta, G., Grasselli, F., Kampermann, H. & Bruß, D. Quantum conference key agreement: a review. *QUTE* **3**, 2000025 (2020).
- Grasselli, F., Murta, G., Kampermann, H. & Bruß, D. Boosting device-independent cryptography with tripartite nonlocality. *Quantum* **7**, 980 (2023).
- Sarkar, S. & Augusiak, R. Self-testing of multipartite Greenberger-Horne-Zeilinger states of arbitrary local dimension with arbitrary number of measurements per party. *Phys. Rev. A* **105**, 032416 (2022).

ACKNOWLEDGEMENTS

We would like to thank Anubhav Chaturvedi, Nicolás Gigena, and Marek Żukowski for insightful discussions. This work is supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No.2022-0-00463, Development of a quantum repeater in optical fiber networks for quantum internet). E.P. acknowledges partial support by NCBiR through QuantEra grant (No. 2/2020), and P.P. acknowledges support by NCN SONATA-BIS grant No. 2017/26/E/ST2/01008.

AUTHOR CONTRIBUTIONS

All authors equally contributed to the conceptualization and preparation of the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s41534-023-00735-3>.

Correspondence and requests for materials should be addressed to Ekta Panwar.

Reprints and permission information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2023