Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing

Cédric Bamps and Stefano Pironio
Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), 1050 Brussels, Belgium
(Received 9 January 2015; published 19 May 2015)

We introduce two families of sum-of-squares (SOS) decompositions for the Bell operators associated with the tilted Clauser-Horne-Shimony-Holt (CHSH) expressions introduced in Acín *et al.* [Phys. Rev. Lett. **108**, 100402 (2012)]. These SOS decompositions provide tight upper bounds on the maximal quantum value of these Bell expressions. Moreover, they establish algebraic relations that are necessarily satisfied by any quantum state and observables yielding the optimal quantum value. These algebraic relations are then used to show that the tilted CHSH expressions provide robust self-tests for any partially entangled two-qubit state. This application to self-testing follows closely the approach of Yang and Navascués [Phys. Rev. A **87**, 050102(R) (2013)], where we identify and correct two nontrivial flaws.

DOI: 10.1103/PhysRevA.91.052111 PACS number(s): 03.65.Ud, 03.67.Mn

I. INTRODUCTION

We consider a bipartite Bell scenario [1] with two binary observables A_0, A_1 for Alice and two binary observables B_0, B_1 for Bob, such that $A_x^2 = \mathbb{I}$, $B_y^2 = \mathbb{I}$, and $[A_x, B_y] = 0$ for all $x, y = 0, 1$.[1] The following family of tilted Clauser-Horne-Shimony-Holt (CHSH) operators for this scenario was introduced in [2]:

$$\mathcal{I}_\alpha = \alpha A_0 + A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1, \tag{1}$$

where $\alpha \in [0,2[$ is a parameter and $\alpha = 0$ corresponds to the CHSH operator. One of our objectives in this article is to derive an upper bound η_α on the maximal quantum expectation value of $\mathcal{I}_\alpha$, that is to show that $\langle \mathcal{I}_\alpha \rangle \leqslant \eta_\alpha$ for all possible quantum states and measurement operators A_x and B_y. This is equivalent to showing that the operator $\overline{\mathcal{I}}_\alpha = \eta_\alpha \mathbb{I} - \mathcal{I}_\alpha$ is positive semidefinite, i.e., $\overline{\mathcal{I}}_\alpha \succeq 0$, for any measurement operators A_x and B_y. This in turn can be proven by providing a set of operators $\{P_i\}$ which are polynomial functions of A_x and B_y such that

$$\overline{\mathcal{I}}_\alpha = \sum_i P_i^\dagger P_i \tag{2}$$

holds for any set of measurement operators satisfying the algebraic properties $A_x^2 = \mathbb{I}$, $B_y^2 = \mathbb{I}$, and $[A_x, B_y] = 0$. Indeed, if $\overline{\mathcal{I}}_\alpha$ is of this form, it is obviously positive semidefinite. A decomposition of the form (2) is called a *sum of squares* and can be defined in full generality for other Bell operators than the ones considered here.

Though it may be difficult to find a sum-of-squares (SOS) decomposition for an arbitrary Bell operator, especially one yielding a tight bound η_α on the maximal quantum violation, once one has been found, verifying that (2) holds, and thus that $\langle \mathcal{I}_\alpha \rangle \leqslant \eta_\alpha$, usually involves only a few simple computations. That is, a SOS provides a simple certificate that $\langle \mathcal{I}_\alpha \rangle \leqslant \eta_\alpha$. Furthermore, the search for optimal SOS can be cast as a series of semidefinite programs (SDP) that turns out to be simply the dual formulation [3] of the SDP hierarchy introduced in [4,5]. Finally, as shown in [6], an optimal SOS, i.e., one for which $\langle \mathcal{I}_\alpha \rangle \leqslant \eta_\alpha$ is a tight bound, provides useful information about the optimal quantum strategy and can find an application in robust self-testing.

Self-testing is the process through which one can guarantee that two devices satisfy certain properties, e.g., that they implement measurements on a quantum state which is close, up to a local isometry, to a given reference state, only by observing the correlations in a Bell experiment [7]. The possibility of self-testing means that the interaction on a classical level with quantum devices can be sufficient to assure users that they indeed hold devices that conform to an ideal specification: as long as the self-testing criteria are satisfied, it is guaranteed that the devices have not malfunctioned or been tampered with. Effectively, this allows the users to treat their devices as black boxes. This is the core idea of device-independent quantum information processing, where self-testing has been used as a primitive to establish schemes for verified quantum computing [8] and cryptographic tasks such as randomness expansion [7,9].

Despite their interest, very few examples of explicit SOS decompositions for Bell operators have been given in the literature. One example is a SOS for the family of "guess your neighbor's input" inequalities introduced in [10]. A second example is a SOS for the CHSH operator appearing in [8], which we recover in this article. Finally, SOS decompositions for the entire family of tilted CHSH operators (1) were proposed in [6]. However, as we point out here, these SOS only hold in the range $\alpha \in [0.156, 1.955]$; outside that range they are not valid SOS due to a sign error that cannot be simply fixed. Furthermore, even within the validity range, these SOS decompositions are not sufficient for the self-testing application proposed in [6] (see Appendix C).

In this article, we introduce two different simple SOS decompositions for the tilted CHSH operators (1) that are valid for the entire range $\alpha \in [0,2[$, including the CHSH case $\alpha = 0$. Our systematic approach to this problem is of independent interest as it can probably be adapted to other Bell operators. We then show, following [11] and [6], how to apply these SOS decompositions to robust self-testing of any partially entangled state. Moreover, we take the self-testing analysis further by

[1] We assume implicitly that Alice's observables are of the form $A_x \otimes \mathbb{I}$ and those of Bob of the form $\mathbb{I} \otimes B_y$.

 ©2015 American Physical Society

showing that the isometry providing a robust self-test for the state also provides a self-test for the action of the measurement operators. Incidentally, we point out and fix a small mistake in [11] concerning the regularization procedure used to define the local isometry used for self-testing.

This article is organized as follows. We first present our SOS decompositions and detail the approach we used to obtain them. We then sketch their application to self-testing, which is comprehensively discussed in Appendix A. The flaws that we identified in [6] and [11] and how our work resolves them is presented in Appendix C.

II. SOS DECOMPOSITIONS FOR TILTED CHSH INEQUALITIES

We first start by reviewing some of the properties of the tilted CHSH expressions $\mathcal{I}_\alpha$. We then introduce the concept of SOS decompositions and derive such decompositions for the tilted CHSH operators.

A. Optimal quantum strategies for $\mathcal{I}_\alpha$

The optimal quantum value for the Bell expressions (1) was computed in [2] by optimizing explicitly over all quantum states and measurements. The optimal value is $I_\alpha^{\max} = \sqrt{8+2\alpha^2}$, to be compared to the classical bound $2+\alpha$. An interesting property of this class of Bell operators is that for all values of $\alpha \in [0,2[$, the maximal quantum value can be achieved by a partially entangled qubit pair

$$|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle \tag{3}$$

with $\alpha \equiv \alpha(\theta) = 2/\sqrt{1+2\tan^2 2\theta}$, effectively covering the full range of partial entanglement in two-qubit states, $\theta \in]0,\pi/4]$. The operators used to achieve this maximal quantum violation are

$$A_0 = \sigma_z, \qquad A_1 = \sigma_x, \tag{4a}$$

$$B_0 = \cos\mu\,\sigma_z + \sin\mu\,\sigma_x, \quad B_1 = \cos\mu\,\sigma_z - \sin\mu\,\sigma_x, \tag{4b}$$

where $\tan\mu = \sin 2\theta$ and $\sigma_{x,z}$ are the x, z Pauli operators.

B. SOS decompositions for Bell operators

Our goal is to find a decomposition as in (2) in terms of a set of polynomials $\{P_i\}$ when the constant term in $\overline{\mathcal{I}}_\alpha$ is the maximal quantum value of the tilted CHSH operator, $\eta_\alpha = I_\alpha^{\max}$. For simplicity, we restrict our search space to the span of a small canonical basis of nine monomials of degree 2,

$$\mathcal{S}_{1+AB} = \{\mathbb{I}, A_0, A_1\} \otimes \{\mathbb{I}, B_0, B_1\}\,. \tag{5}$$

To simplify the search, we will later pick a different basis of this vector space of polynomials, $\{R_i\}_i$. Thus, the operators P_i are decomposed as $P_i = q_i^\mu R_\mu$ (using implicit summation on repeated indices). The expression of $\overline{\mathcal{I}}_\alpha$ as an SOS (2) then becomes

$$\overline{\mathcal{I}}_\alpha = R_\mu^\dagger q_i^{\mu *} q_i^\nu R_\nu \equiv R_\mu^\dagger M^{\mu\nu} R_\nu\,. \tag{6}$$

If q_i^ν is now seen as the ith component of a vector $\mathbf{q}^\nu$, the Hermitian matrix M is then the Gram matrix of this set of nine vectors and is therefore positive semidefinite. The converse is also true: if M is positive semidefinite, there exists a (nonunique) set of vectors $\{\mathbf{q}^\nu\}$ such that the components $M^{\mu\nu}$ are the Hermitian products $(\mathbf{q}^\mu,\mathbf{q}^\nu) = q_i^{\mu *} q_i^\nu$, and therefore any operator of the form of the right-hand side of (6) with $M \succeq 0$ is a sum of squares. A set of such vectors $\{\mathbf{q}^\nu\}$ is given by the columns of any matrix square root of M, such as its Cholesky decomposition if it is nonsingular.

We are now looking for a positive semidefinite matrix M such that (6) holds. This equation imposes linear constraints on M. Indeed, we can decompose both sides of the equality $\overline{\mathcal{I}}_\alpha = M^{\mu\nu} R_\mu^\dagger R_\nu$ in a basis of the quadratic products of all elements in $\mathcal{S}_{1+AB}$, which is of size 25 rather than 81 due to the algebraic relations satisfied by the measurement operators. A canonical basis for these products is

$$\mathcal{S}_{1+AB}^2 = \{\mathbb{I}, A_0, A_1, A_0A_1, A_1A_0\} \otimes \{\mathbb{I}, B_0, B_1, B_0B_1, B_1B_0\}\,. \tag{7}$$

Writing $R_\mu^\dagger R_\nu = F_{\mu\nu}^i E_i$ where E_i runs through S_{1+AB}^2 and each F^i is a matrix of complex coefficients, and likewise $\overline{\mathcal{I}}_\alpha = s^i E_i$, the SOS condition (6) reduces to

$$s^i = \mathrm{Tr}(M^\dagger F^i) \quad (i = 1, \ldots, 25)\,. \tag{8}$$

We are thus left with a set of 25 linear equality constraints on M as well as the positive semidefiniteness constraint $M \succeq 0$. This is a semidefinite programming feasibility problem, which can be approached with numerical tools such as SeDuMi [12].

However, while we could attempt to recover the exact analytical expression that the numerical solution approximates, this will not be a good approach for a continuous class of Bell operators. We will thus tackle this problem analytically, and this requires that we simplify the problem as much as possible. One first simplification comes from our knowledge of a state and measurements which achieve the quantum bound. One such system is specified in Eqs. (3) and (4a), consisting in the partially entangled qubit pair $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ with spin measurements along given axes. Because this strategy achieves the quantum bound $I_\alpha^{\max}$, the expectation value of $\overline{\mathcal{I}}_\alpha$ vanishes. As a consequence, any SOS decomposition for $\overline{\mathcal{I}}_\alpha$ of the form (2) must have each of its terms vanish in expectation as well. Hence, a valid SOS decomposition for $\overline{\mathcal{I}}_\alpha$ must be made up of terms for which $P_i\,|\psi\rangle = 0$ in this maximally violating quantum system. This last equation defines four constraints that all P_i must obey, one per basis vector of the Hilbert space. Indeed, writing the most general P in our search space as $\mathbf{r}\cdot\mathbf{V}$ where

$$\mathbf{V} = (\mathbb{I}, A_0, A_1, B_0, B_1, A_0B_0, A_0B_1, A_1B_0, A_1B_1) \tag{9}$$

and demanding that the four components of $P\,|\psi\rangle = P(\cos\theta\,|00\rangle + \sin\theta\,|11\rangle)$ [with the observables specified in (4a)] vanish, we find four independent linear constraints on the vector $\mathbf{r}$. We thus find that the space of candidates P_i is spanned by the following five operators:

$$Z_\mathrm{A} - Z_\mathrm{B}, \tag{10a}$$

$$\mathbb{I} - Z_\mathrm{A}Z_\mathrm{B}, \tag{10b}$$

$$cX_\mathrm{A} - sZ_\mathrm{A}X_\mathrm{B} - X_\mathrm{A}Z_\mathrm{B}, \tag{10c}$$

$$cX_\mathrm{B} - sX_\mathrm{A}Z_\mathrm{B} - Z_\mathrm{A}X_\mathrm{B}, \tag{10d}$$

$$sX_\mathrm{A}X_\mathrm{B} - Z_\mathrm{A}Z_\mathrm{B} + cZ_\mathrm{A}, \tag{10e}$$

where $c = \cos 2\theta$, $s = \sin 2\theta$, and the Z and X operators are defined as

$$Z_{\mathrm{A}} = A_0, \qquad X_{\mathrm{A}} = A_1, \tag{11a}$$

$$Z_{\mathrm{B}} = \frac{B_0 + B_1}{2\cos\mu}, \quad X_{\mathrm{B}} = \frac{B_0 - B_1}{2\sin\mu}. \tag{11b}$$

It is easily verified that these five operators indeed vanish in the explicit two-qubit system we considered, as Z and X are then the Pauli operators.

This first step lets us write the P_i polynomials as linear combinations of five operators instead of nine, hence the M matrix in our SDP feasibility problem is now 5×5.

One further simplification comes from exploiting the symmetry of the tilted CHSH operator to impose a similar symmetry on its SOS decompositions. The effect of symmetries on SOS decompositions has been studied in the case of polynomials of commutative variables in [13], and the following takes inspiration from those results. We observe that changing the sign of $A_1 \to -A_1$ and swapping $B_0 \leftrightarrow B_1$ leaves $\mathcal{I}_\alpha$ (and therefore $\overline{\mathcal{I}}_\alpha$) invariant. This transformation induces a representation of the cyclic group C_2 on the vector space of operators $\mathrm{span}(\mathcal{S}_{1+AB})$. Let $\sigma \in \mathrm{End}\,(\mathrm{span}(\mathcal{S}_{1+AB}))$ be the endomorphism representing the transformation. Due to the invariance of the tilted CHSH operator, the five-dimensional subspace spanned by operators (10) is itself invariant under σ by definition. Therefore, we separate this subspace as a direct sum of irreducible representation subspaces, all of dimension 1 according to the representation theory of cyclic groups. We then choose our basis operators $\{R_i\}_{i=1}^5$ to be the basis elements associated with such a decomposition. This means that σ acts on this basis as $\sigma(R_i) = \pm R_i$, depending on i.

We now apply this symmetry transformation to both sides of (2):

$$\overline{\mathcal{I}}_\alpha = \sigma(\overline{\mathcal{I}}_\alpha) = \sigma(R_\mu)^\dagger M^{\mu\nu}\sigma(R_\nu) = R_\mu^\dagger M'^{\mu\nu} R_\nu\,, \tag{12}$$

where $M'^{\mu\nu} = \pm M^{\mu\nu}$ depending on the sign brought by the transformation of the basis operators. This means that M' represents a new SOS decomposition for $\overline{\mathcal{I}}_\alpha$. Moreover, because convex combinations of SOS decompositions are also valid SOS decompositions of the same operator, a third SOS decomposition is found: $M^{(\mathrm{S})} = (M + M')/2$. This last SOS has the property of being invariant under the symmetry transformation.

While asymmetric SOS may still exist, this result is useful because it lets us focus on symmetric decompositions, which have a smaller number of degrees of freedom. Indeed, because elements in M' and M only differ by their sign, the symmetrization of M to $M^{(\mathrm{S})}$ will take to zero the elements that change sign. The elements in question correspond to indices (μ,ν) such that R_μ and R_ν span representation subspaces of different irreducible representations of C_2. As a result, the symmetrized SOS matrix $M^{(\mathrm{S})}$ is block-diagonal, with one block associated to each of the two irreducible representations.

Considering the discussion thus far, we now choose a basis for the subspace containing the SOS polynomials. The basis we choose is $\{R_i \equiv \mathbf{r}_i \cdot \mathbf{V}\}$ where the $\mathbf{r}_i$ vectors are defined as such (we label the columns with the operators defining $\mathbf{V}$ for convenience):

$$\begin{array}{cccccccccc}
 & \mathbb{I} & A_0 & A_1 & B_0 & B_1 & A_0B_0 & A_0B_1 & A_1B_0 & A_1B_1 \\
\mathbf{r}_1 = & \Big(0 & \frac{-2}{\sqrt{1+s^2}} & 0 & 1 & 1 & 0 & 0 & 0 & 0\Big), \\
\mathbf{r}_2 = & \Big(\frac{-2}{\sqrt{1+s^2}} & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0\Big), \\
\mathbf{r}_3 = & \Big(\frac{-2}{\sqrt{1+s^2}} & 0 & 0 & c & c & 0 & 0 & 1 & -1\Big), \\
\mathbf{r}_4 = & \Big(0 & 0 & \frac{-2}{\sqrt{1+s^2}} & 1 & -1 & 0 & 0 & c & c\Big), \\
\mathbf{r}_5 = & \Big(0 & 0 & \frac{-2c}{\sqrt{1+s^2}} & 0 & 0 & 1 & -1 & 1 & 1\Big).
\end{array} \tag{13}$$

It is easily checked that these basis operators separate the space in two isotypical subspaces, i.e., subspaces that fall under the same irreducible representation of the cyclic group: $R_{1,2,3}$ are invariant under the symmetry transformation of $\mathcal{I}_\alpha$, while $R_{4,5}$ change sign. The block structure of symmetric SOS matrices is therefore $3 \oplus 2$, where the first block corresponds to the trivial representation and the second to the parity representation where the group generator is represented by -1: we have $\sigma(R_i) = R_i$ for $i = 1,2,3$ and $\sigma(R_i) = -R_i$ for $i = 4,5$.

We now examine the problem of finding SOS decompositions with $\alpha = 0$, where $\mathcal{I}_0$ is the CHSH operator, and with $\alpha = \alpha(\pi/8)$.

1. CHSH case: $\alpha = 0$

We first look at the determination of SOS decompositions in the simplest case, where $\alpha = 0$. Without yet taking symmetry into account, the linear constraints imposed on M by Eq. (8) imply (omitting the lower triangular part given by hermiticity)

$$M = \frac{1}{2\sqrt{2}}\begin{pmatrix} \lambda & 0 & 0 & \delta & 0 \\ & \gamma & q & 0 & -\delta/2 \\ & & t & 0 & -\delta/2 \\ & & & \mu & 0 \\ & & & & q \end{pmatrix} \tag{14}$$

with $q = 1 - \lambda - \gamma$ and $t = \lambda + \gamma - \mu$. Thus, M depends on four parameters, three of which are real due to hermiticity. The fourth parameter, δ, can be taken to 0 by the symmetry argument given above. We see that, in this specific case, the $1 \oplus 2 \oplus 1 \oplus 1$ block structure of a symmetric M goes further than what is imposed by the symmetry of $\mathcal{I}_\alpha$. This is not surprising, as the CHSH operator, lacking a marginal term, is more symmetric than the general I_α operator. This makes it straightforward to impose positive semidefiniteness: a necessary and sufficient condition is the positive semidefiniteness of the blocks. We find the conditions

$$\lambda,\mu,q,t \geqslant 0\,, \tag{15}$$

$$\lambda t - q^2 \geqslant 0\,. \tag{16}$$

We therefore end up with a simple description of the full solution set of symmetric SOS decompositions of $\overline{\mathcal{I}}_0$ in $\mathcal{S}_{1+AB}$, up to the computation of a square root for M to get the actual polynomials P_i in (2). We represent this solution set in terms of λ, μ and q in Fig. 1.

In this solution set, the extremal points are the most interesting as they generate the entire set by convex combinations. Here, the extremal points are the five vertices of the set and the smooth quadratic surface resulting from inequality (16). Because of their situation at the intersection of inequality constraints, the M matrices at the five vertices are of low rank, which eases the determination of a square root. Those distinguished extremal points are listed in Table I. We note that the first four vertex SOS in the table are equivalent up to multiplication on the left by a dichotomic operator on one or two of the operators that are squared in the sum. For instance, the identity $R_2 = A_0 R_1$ implies that $R_2^2 = R_1^2$, which means that the SOS C_1 and C_2 are equivalent.

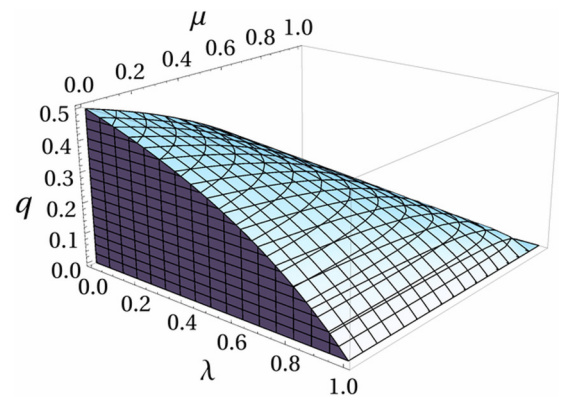

FIG. 1. (Color online) Solution set for symmetric SOS decompositions for the CHSH operator in $\mathcal{S}_{1+AB}$.

We reproduce here two SOS decompositions of $\overline{\mathcal{I}}_0$ resulting from those extremal points:

$$\overline{\mathcal{I}}_0 = \frac{1}{4\sqrt{2}}\left[\overline{\mathcal{I}}_0^2 + 2(Z_A X_B + X_A Z_B)^2\right] \tag{17}$$

$$\overline{\mathcal{I}}_0 = \frac{1}{\sqrt{2}}[(-Z_A + Z_B)^2 + (-X_A + X_B)^2], \tag{18}$$

where $Z_A = A_0$, $X_A = A_1$, $Z_B = (B_0 + B_1)/\sqrt{2}$, and $X_B = (B_0 - B_1)/\sqrt{2}$. We note that the decomposition (18), which we denote as C_4 in Table I, also appears in [8].

Two additional SOS decompositions for CHSH are also given in Appendix B.

2. $\theta = \pi/8$ case

Next, we choose the (arbitrary) value of $\theta = \pi/8$. The equality constraints (8) give to the SOS matrix the following form:

$$M = \frac{\sqrt{3}}{8\sqrt{2}}\begin{pmatrix} \beta & \frac{-1}{\sqrt{2}} & \frac{3}{\sqrt{2}}\gamma & 3\delta & 0 \\ & \frac{5}{3} - \beta + \frac{1}{2}\gamma & \frac{1}{3} - 2\gamma & -\sqrt{2}\delta & -\delta \\ & & 2 + 3\gamma - \lambda & \sqrt{2}\delta & -2\delta \\ & & & \lambda & \frac{-\sqrt{2}}{3} - \sqrt{2}\gamma \\ & & & & \frac{2}{3} - \gamma \end{pmatrix}, \tag{19}$$

where, again, δ can be set to zero by symmetry to give M a block-diagonal structure.

Contrary to the CHSH matrix, the block structure in this case is coarser with fewer, larger blocks, which results in more nonlinear positive semidefiniteness constraints. The positive semidefiniteness of M is checked by using a generalized form of Sylvester's criterion, namely that a matrix is positive semidefinite if and only if all of its principal minors (submatrices obtained by jointly eliminating lines and columns of the same indices), including the matrix itself, have a nonnegative determinant [14]. The solution set is visualized as a three-dimensional convex region in Fig. 2, delimited by a quadratic surface and a cubic surface.

We identify on Fig. 2 two points that stand out, namely the two cusps at the intersection of the two surfaces delimiting the region. Their coordinates are found to be $(\beta,\gamma,\lambda) = (1/2,-1/3,0)$ and $(3/2,1/3,8/3)$. Both blocks of M have rank 1 at these points, which eases the computation of square roots N that describe the SOS polynomials. We find respectively

$$N_1 = \sqrt{\frac{\sqrt{3}}{8\sqrt{2}}}\begin{pmatrix} 1/\sqrt{2} & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \tag{20}$$

$$N_2 = \sqrt{\frac{\sqrt{3}}{8\sqrt{2}}}\begin{pmatrix} -\sqrt{\frac{3}{2}} & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & 0 & 0 \\ 0 & 0 & 0 & -2\sqrt{\frac{2}{3}} & \frac{1}{\sqrt{3}} \end{pmatrix}. \tag{21}$$

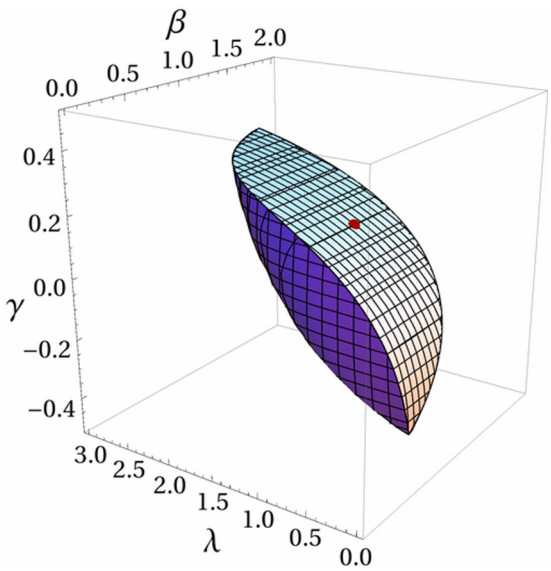

FIG. 2. (Color online) Solution set for symmetric SOS decompositions for $\mathcal{I}_{\alpha(\pi/8)}$ in $\mathcal{S}_{1+AB}$. This set is delimited by a quadratic surface (invariant along β) and a cubic surface. Yang and Navascués' SOS [6] is represented as a red dot.

The rows in these matrices give us the coefficient vectors $\mathbf{q}_i$ for two explicit SOS decompositions of $\overline{\mathcal{I}}_{\alpha(\pi/8)}$.

3. General tilted CHSH

The general approach is the same as above: first, the linear constraints (8) are imposed, and imposing symmetry leaves us with three real degrees of freedom. The positive semidefiniteness of the blocks of M is then enforced by applying the generalized Sylvester's criterion [14]. This amounts to one cubic, four quadratic, and five linear inequalities. For a given value of α, the solution set is readily visualized as a convex set in $\mathbb{R}^3$.

In the previous section, we examined the case of $\alpha = \alpha(\pi/8)$ and identified two extremal points in the solution set where each block of the SOS matrix M is of rank 1. When we carry out the explicit expansion of the sums of squares, these decompositions hint at an easy generalization to all values of α for both points. This leads us to the two SOS decompositions that follow. Let us first define the following permutations of the CHSH operator:

$$\mathcal{S}' = A_0(B_0 - B_1) + A_1(B_0 + B_1)\,, \tag{22}$$

$$\mathcal{S}'' = A_0(B_0 + B_1) - A_1(B_0 - B_1)\,, \tag{23}$$

$$\mathcal{S}''' = A_0(B_0 - B_1) - A_1(B_0 + B_1)\,. \tag{24}$$

The two decompositions we find are the following:

$$\overline{\mathcal{I}}_\alpha = \frac{1}{2I_\alpha^{\max}}\left[\overline{\mathcal{I}}_\alpha^2 + (\alpha A_1 - \mathcal{S}')^2\right] \tag{25}$$

and

$$\overline{\mathcal{I}}_\alpha = \frac{1}{2I_\alpha^{\max}}\left[\left(2A_0 - I_\alpha^{\max}\frac{B_0 + B_1}{2} + \frac{\alpha}{2}\mathcal{S}''\right)^2 + \left(2A_1 - I_\alpha^{\max}\frac{B_0 - B_1}{2} + \frac{\alpha}{2}\mathcal{S}'''\right)^2\right]. \tag{26}$$

The two SOS decompositions given in the CHSH case (17), (18) are limiting cases of (25) and (26). Independently of the way we arrived at (25) and (26), it is readily verified that they correspond to valid SOS.

III. APPLICATION TO SELF-TESTING

We conclude by discussing the application of the above results to self-testing. We know that measuring the state $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ with the observables (4a) leads to the maximal value $I_\alpha^{\max}$ of the Bell expression $\mathcal{I}_\alpha$. We say that this Bell expression provides a robust self-test for this particular reference state and reference observables if the converse also holds, in a noise-tolerant way—that is, if an expected value of $\mathcal{I}_\alpha$ close to the maximum $I_\alpha^{\max}$ necessarily corresponds to measurements involving a state and observables that are close to the reference, up to a local isometry. More precisely, we show, following the framework of [11] and [6], the following. Let $\langle\tilde{\mathcal{I}}_\alpha\rangle$ be the expectation value of the Bell expression $\mathcal{I}_\alpha$ obtained by measuring a physical state $|\tilde{\psi}\rangle$ with physical observables $\tilde{A}_x$ and $\tilde{B}_y$. Let $|\psi\rangle$ and A_x and B_y be the reference state and reference observables corresponding to the optimal quantum strategies for $\mathcal{I}_\alpha$ defined in Sec. II A. Then if $\langle\tilde{\mathcal{I}}_\alpha\rangle \geqslant I_\alpha^{\max} - \epsilon$, there exists a local isometry $\Phi = \Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}$ and a state $|\mathrm{junk}\rangle$ such that

$$\|\Phi(\tilde{A}_x \otimes \tilde{B}_y\,|\tilde{\psi}\rangle) - |\mathrm{junk}\rangle \otimes (A_x \otimes B_y)\,|\psi\rangle\| \leqslant \epsilon' \tag{27}$$

for $x,y \in \{-1,0,1\}$, where the subscript -1 refers to the identity operator and where $\epsilon' = O(\sqrt{\epsilon})$. The precise relation between ϵ and ϵ' is given in Appendix A.

The case of the CHSH inequality ($\alpha = 0$) was already considered in [11], where Eq. (27) was obtained but with a weaker $\epsilon' = O(\epsilon^{1/4})$ robustness. Equation (27) in the case $x,y = -1$ for arbitrary values of $\alpha \in [0,2[$, corresponding to a self-test of any partially entangled state (but not of the associated observables), was considered in [6], where the authors showed that the use of SOS decompositions could in principle lead to an optimal $\epsilon' = O(\sqrt{\epsilon})$ robustness. This conclusion, however, does not follow from the analysis presented in [6] due to different shortcomings in the derivation of intermediate results (see Appendix C for details). Here we resolve these shortcomings, thanks in particular to the two SOS decompositions (25) and (26), and establish the robust self-testing conditions (27), thus further extending the analysis in [6] to the self-testing of the observables (4a) in addition to the state (3).

Following closely [6], we now sketch the proof of the robust self-testing result (27) and refer to Appendix A for details. The proof proceeds in three steps. First, we define as in [11] the isometry appearing in (27) as the successive action of a set of gates, represented as a circuit in Fig. 3, acting on the initial state $|00\rangle \otimes |\tilde{\psi}\rangle$. The gates are defined in terms of the measurement operators $\tilde{A}_x$ and $\tilde{B}_y$ as an inversion of (4a) in an attempt to recover the behavior of the Pauli operators. Specifically, we define as in (11a)

$$\tilde{Z}_{\mathrm{A}} = \tilde{A}_0, \qquad \tilde{X}_{\mathrm{A}} = \tilde{A}_1, \tag{28a}$$

$$\tilde{Z}_{\mathrm{B}} = \frac{\tilde{B}_0 + \tilde{B}_1}{2\cos\mu}, \quad \tilde{X}_{\mathrm{B}} = \frac{\tilde{B}_0 - \tilde{B}_1}{2\sin\mu}\,. \tag{28b}$$

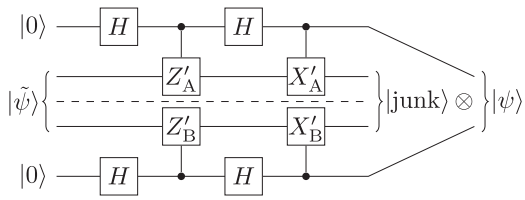

FIG. 3. The local isometry used to locate the partially entangled qubit pair in the physical system. The dashed line shows the physical separation between Alice (top) and Bob (bottom).

Because we need unitary gates in the isometry, a regularization procedure is applied to normalize the eigenvalues of the operators: we define $Z'_{\mathrm{B}} = \tilde{Z}^*_{\mathrm{B}}|\tilde{Z}^*_{\mathrm{B}}|^{-1}$ where $\tilde{Z}^*_{\mathrm{B}}$ is $\tilde{Z}_{\mathrm{B}}$ with its zero eigenvalues changed to 1. The same procedure is applied to define X'_{B}. Alice's operators are unchanged because they are already unitary: $Z'_{\mathrm{A}} = \tilde{Z}_{\mathrm{A}}$ and $X'_{\mathrm{A}} = \tilde{X}_{\mathrm{A}}$. As a side note, we point out a slight mistake in [11] concerning the above regularization procedure; see Appendix C.

Second, we observe, as mentioned earlier and as pointed out in [6], that the existence of a SOS decomposition for $\overline{\mathcal{I}}_\alpha$ of the form (2) implies that any state $|\tilde{\psi}\rangle$ and operators $\tilde{A}_x$ and $\tilde{B}_y$ achieving the quantum bound $I_\alpha^{\max}$ must obey the relations $\tilde{P}_i\,|\tilde{\psi}\rangle = 0$. Moreover, this property is robust: if instead the expectation value is $\langle\tilde{\mathcal{I}}_\alpha\rangle = I_\alpha^{\max} - \epsilon$, then we have $\|\tilde{P}_i\,|\tilde{\psi}\rangle\| \leqslant \sqrt{\epsilon}$. This observation applied to the two SOS (25) and (26) implies the following identities up to robust error terms:

$$(\tilde{Z}_{\mathrm{A}} - \tilde{Z}_{\mathrm{B}})\,|\tilde{\psi}\rangle = 0\,, \tag{29a}$$

$$(\sin\theta\,\tilde{X}_{\mathrm{A}}(\mathbb{I} + \tilde{Z}_{\mathrm{B}}) - \cos\theta\,\tilde{X}_{\mathrm{B}}(\mathbb{I} - \tilde{Z}_{\mathrm{A}}))\,|\tilde{\psi}\rangle = 0\,, \tag{29b}$$

$$(\tilde{Z}_{\mathrm{A}}\tilde{X}_{\mathrm{A}} - \tilde{X}_{\mathrm{A}}\tilde{Z}_{\mathrm{A}})\,|\tilde{\psi}\rangle = 0\,. \tag{29c}$$

For instance, identity (29a) in the case $\alpha = 0$ is easily seen to follow from the term $P_1 = (-Z_A + Z_B)$ present in the SOS decomposition (18). The three identities (29) for arbitrary α follow in a similar, though more involved, manner from the two SOS (25) and (26); see Appendix A.

The third step of the proof then examines the action of the isometry on a state and observables satisfying the algebraic relations (29). It establishes that in this case the relations (27) necessarily hold between the inputs and outputs of the isometry. As in [6], a lengthy series of triangle inequalities is needed to go from the SOS bounds on $\|P_i\,|\tilde{\psi}\rangle\|$ to the robustness bounds for (29) and finally to (27). We refer to Appendix A for the derivation, where explicit bounds in $O(\sqrt{\epsilon})$ for all the identities in (27) are determined.

IV. DISCUSSION

In this work, we provided tools to simplify the search for sums-of-squares decompositions for Bell operators, exploiting their symmetries and the knowledge of systems that maximally violate the associated Bell inequalities. We applied this approach to find two SOS decompositions for the family of tilted CHSH inequalities of [2] (as well as some extra decompositions in the special case of the CHSH inequality). We made use of these new SOS decompositions to complete and extend the proof of Yang and Navascués [6] by showing that a close-to-maximal quantum violation of a tilted CHSH inequality provides a robust self-test for the reference state and measurement operators associated with the inequality.

The general form $C\sqrt{\epsilon}$ of our distance bounds is optimal in the noise parameter ϵ in the sense that a larger exponent for ϵ would contradict the hypothesis $\langle\overline{\mathcal{I}}_\alpha\rangle \leqslant \epsilon$. These distance bounds, though, become very sensitive to noise as the entanglement diminishes. This is not surprising, as taking the entanglement parameter θ close to zero takes the extremal quantum behavior for the $\mathcal{I}_\alpha$ inequality closer to the local set.

The reference systems for the tilted CHSH inequalities are particularly relevant to randomness generation, as explained in [2]. Our self-testing statement may therefore be useful in establishing device-independent protocols using partially entangled states as a resource for randomness expansion.

We hope that a similar approach to finding SOS decompositions for Bell inequalities will find further applications in robust property testing in different systems, for instance with higher-dimensional reference Hilbert spaces.

ACKNOWLEDGMENTS

We acknowledge financial support from the EU project QALGO, from the F.R.S.-FNRS under the project DIQIP, and from the Brussels-Capital Region through a BB2B grant. S.P. was supported by Fonds de la Recherche Scientifique F.R.S.-FNRS (Belgium). C.B. acknowledges funding from the F.R.S.-FNRS through a Research Fellowship.

APPENDIX A: ROBUST SELF-TEST

1. Introduction

In this section, we show how our SOS results can be used to provide a robust self-test of the systems that maximally violate the $\mathcal{I}_\alpha$ inequalities. We work in the following setting: two isolated parties, Alice and Bob, hold black boxes that each take one of two inputs, respectively x and y, in $\{0,1\}$, and each return one of two outputs, a and b, in $\{+1,-1\}$. They wish to make sure that their boxes share the partially entangled qubit pair $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ and that the observables characterizing their measurements on their share of the state are given in terms of the Pauli operators as

$$A_0 = \sigma_z, \qquad A_1 = \sigma_x, \tag{A1a}$$

$$B_0 = \cos\mu\,\sigma_z + \sin\mu\,\sigma_x, \qquad B_1 = \cos\mu\,\sigma_z - \sin\mu\,\sigma_x \tag{A1b}$$

with $\tan\mu = \sin 2\theta$. In reality, the boxes hold the physical state $|\tilde{\psi}\rangle$ and the observables are the Hermitian and dichotomic (i.e., of eigenvalues ± 1) operators $\tilde{A}_x$ and $\tilde{B}_y$—this is general because there is no assumption made on the dimensionality of the Hilbert space, which can thus be extended to purify the state and make the measurements projective.

We follow the framework of McKague *et al.* [11] and say that a Bell expression provides a robust self-test for a reference system if, for a violation of the corresponding Bell inequality that is ϵ-close to the quantum maximum (we say that the system satisfies the self-testing criterion), the state and measurements that give rise to this violation are close to the reference, with the error vanishing as ϵ goes to zero.

Formally, this is stated as the existence of a local isometry with respect to Alice and Bob that takes $|\tilde{\psi}\rangle$ and the action of their observables $\tilde{A}_x$ and $\tilde{B}_y$ to a system close to the reference $|\psi\rangle$ and A_x, B_y, in tensor product with uncorrelated degrees of freedom. The precise mathematical statement is the following: assuming that the self-testing criterion holds, there exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$ and a state $|\text{junk}\rangle$ such that

$$\|\Phi(\tilde{A}_x \otimes \tilde{B}_y\,|\tilde{\psi}\rangle) - |\text{junk}\rangle \otimes (A_x \otimes B_y)\,|\psi\rangle\| \leqslant e_{xy}(\epsilon) \quad \text{(A2)}$$

for all $x,y \in \{-1,0,1\}$ (where operators with subscript -1 refer to the identity), and $\lim_{\epsilon\to 0} e_{xy}(\epsilon) = 0$. This is understood as meaning that there exists a procedure (that need not be accessible experimentally) that Alice and Bob can follow locally to perform a change of basis after which the reference state and operators (or something close) are found in a four-dimensional subspace of the global Hilbert space.

We show in this section a robust self-test for the ideal reference system highlighted above for $\mathcal{I}_\alpha$ for any $\alpha \in [0,2[$, with self-testing criterion $\langle\tilde{\psi}|\,\mathcal{I}_\alpha\,|\tilde{\psi}\rangle = I^{\max} - \epsilon$ (with $\mathcal{I}_\alpha$ expressed in terms of $\tilde{A}_x$ and $\tilde{B}_y$), leading to explicit self-testing bounds $e_{xy} \in O(\sqrt{\epsilon})$. This result uses the same techniques as [6] to achieve the self-test of the state [statement (A2) for $x = y = -1$] and extends the reasoning to the self-test of operators.

Following [6,11], we define the following operators, essentially an inversion of (A1) for the physical operators:

$$\tilde{Z}_A = \tilde{A}_0, \qquad \tilde{X}_A = \tilde{A}_1, \quad \text{(A3a)}$$

$$\tilde{Z}_B = \frac{\tilde{B}_0 + \tilde{B}_1}{2\cos\mu}, \quad \tilde{X}_B = \frac{\tilde{B}_0 - \tilde{B}_1}{2\sin\mu}. \quad \text{(A3b)}$$

We regularize these operators into unitaries to use them in the isometry. The procedure is as follows: start from the physical observable, for example $\tilde{Z}_B$, and change all 0 eigenvalues to 1, resulting in a new Hermitian operator Z_B^*. Then, normalize the eigenvalues by defining $Z'_B = \tilde{Z}_B^*|\tilde{Z}_B^*|^{-1}$. This last operator is by construction unitary, self-adjoint, commutes with $\tilde{Z}_B$, and has the property that $Z'_B\tilde{Z}_B = |\tilde{Z}_B|$. Similarly, we define X'_B, Z'_A and X'_A, noting that Alice's regularized X'_A and Z'_A operators actually coincide with the physical operators $\tilde{X}_A$ and $\tilde{X}_B$.

We now define the self-testing isometry by representing it in circuit form in Fig. 3. In general, the action of the isometry on the physical state $|\tilde{\psi}\rangle$ is

$$\begin{aligned}\Phi(|\tilde{\psi}\rangle) = \tfrac{1}{4}[&(\mathbb{I} + Z'_A)(\mathbb{I} + Z'_B)\,|\tilde{\psi}\rangle\,|00\rangle \\ &+ X'_A(\mathbb{I} - Z'_A)(\mathbb{I} + Z'_B)\,|\tilde{\psi}\rangle\,|10\rangle \\ &+ X'_B(\mathbb{I} + Z'_A)(\mathbb{I} - Z'_B)\,|\tilde{\psi}\rangle\,|01\rangle \\ &+ X'_A X'_B(\mathbb{I} - Z'_A)(\mathbb{I} - Z'_B)\,|\tilde{\psi}\rangle\,|11\rangle]\,. \end{aligned} \quad \text{(A4)}$$

In this form, the motivation for this isometry is readily understood. In the reference system with state $|\psi\rangle$ and operators (A1), the $\tilde{X}$ and $\tilde{Z}$ operators above (and their regularizations) are the Pauli operators σ_x and σ_z. Then, $\Phi(|\psi\rangle)$ is easily seen to be $|00\rangle\,|\psi\rangle$, where the partially entangled qubit pair $|\psi\rangle$ has been extracted onto the ancilla qubits, leaving behind the state $|00\rangle$ in the physical register, unentangled with the ancilla. Moreover, by manipulating (A4) using the operators' properties, it is easily seen in this ideal setting that acting on the input with the measurement operators is equivalent to acting on the corresponding ancillae with the reference operators.

Our goal is to extend this statement to all other systems that maximally violate the $\mathcal{I}_\alpha$ inequality, and show its robustness to noise by deriving (A2). To do this, we need to show that the self-testing criterion implies some robust properties on the action of the physical operators on the state.

2. Application of our SOS decompositions to robust self-testing

We first start by reformulating our two SOS decompositions and show that, even though they contain only four independent terms, they still provide a way to test the entire five-dimensional space of relations that we defined as we identified candidates for SOS decompositions in Eqs. (10). Defining the following polynomials in A_x, B_y:

$$S_1 = \overline{\mathcal{I}}_\alpha, \quad \text{(A5a)}$$

$$S_2 = \alpha A_1 - \mathcal{S}', \quad \text{(A5b)}$$

$$S_3 = 2A_0 - I_\alpha^{\max}\frac{B_0 + B_1}{2} + \frac{\alpha}{2}\mathcal{S}'', \quad \text{(A5c)}$$

$$S_4 = 2A_1 - I_\alpha^{\max}\frac{B_0 - B_1}{2} + \frac{\alpha}{2}\mathcal{S}''', \quad \text{(A5d)}$$

with

$$\mathcal{S}' = A_0(B_0 - B_1) + A_1(B_0 + B_1)\,, \quad \text{(A6)}$$

$$\mathcal{S}'' = A_0(B_0 + B_1) - A_1(B_0 - B_1)\,, \quad \text{(A7)}$$

$$\mathcal{S}''' = A_0(B_0 - B_1) - A_1(B_0 + B_1)\,, \quad \text{(A8)}$$

the two SOS decompositions of $\overline{\mathcal{I}}_\alpha$ are then

$$\overline{\mathcal{I}}_\alpha = \frac{1}{2I_\alpha^{\max}}\left(S_1^2 + S_2^2\right) = \frac{1}{2I_\alpha^{\max}}\left(S_3^2 + S_4^2\right). \quad \text{(A9)}$$

We can also express the S_i polynomials as $\mathbf{s}_i \cdot \mathbf{V}$ with $\mathbf{V}$ defined in (9) and $\mathbf{s}_i$ expressed in terms of the basis vectors (13):

$$\mathbf{s}_1 = c\,\mathbf{r}_1 - \mathbf{r}_2 - \mathbf{r}_3, \quad \text{(A10a)}$$

$$\mathbf{s}_2 = -\mathbf{r}_5\,, \quad \text{(A10b)}$$

$$\mathbf{s}_3 = -\sqrt{1+s^2}\,\mathbf{r}_1 + \frac{c}{\sqrt{1+s^2}}(\mathbf{r}_2 - \mathbf{r}_3)\,, \quad \text{(A10c)}$$

$$\mathbf{s}_4 = \frac{-2}{\sqrt{1+s^2}}\,\mathbf{r}_4 + \frac{c}{\sqrt{1+s^2}}\,\mathbf{r}_5\,. \quad \text{(A10d)}$$

The four S_i polynomials above do not span the entire candidate subspace span($\{R_i\}$) that we identified in Eqs. (10). Indeed, while s_2 and s_4 generate the parity isotypical subspace spanned by r_4 and r_5, the other isotypical subspace is not spanned by the other two vectors. For example, r_3 cannot be decomposed in terms of s_1 and s_3 alone. We note however that left multiplication by A_1 takes an operator from the parity to the identity representation subspaces and vice versa. In fact, the simple relation $R_3 = A_1 R_4$ holds. Because R_3 is not a linear combination of the S_i operators while R_4 is, we define $S_5 = R_3$ (and $\mathbf{s}_5 = \mathbf{r}_3$), which is then expressed in terms of the

other four S_i as

$$S_5 = A_1\left(\frac{-c}{2}S_2 - \frac{\sqrt{1+s^2}}{2}S_4\right). \tag{A11}$$

Suppose now that the physical state $|\tilde{\psi}\rangle$ and observables $\tilde{A}_x, \tilde{B}_y$ satisfy the self-testing criterion with error ϵ, i.e., the expectation value $\langle\tilde{\mathcal{I}}_\alpha\rangle$ for the $\mathcal{I}_\alpha$ Bell expression is such that $\langle\tilde{\mathcal{I}}_\alpha\rangle = I_\alpha^{\max} - \epsilon$. Denote as $\mathcal{I}_\alpha$ the Bell operator defined in terms of the observables $\tilde{A}_x$ and $\tilde{B}_y$, and let $\{P_i\}$ be a set of polynomials in these observables such that $I_\alpha^{\max}\mathbb{I} - \mathcal{I}_\alpha \equiv \overline{\mathcal{I}}_\alpha = \sum_i P_i^\dagger P_i$. Then, the self-testing criterion directly implies the bounds $\langle\tilde{\psi}|\, P_i^\dagger P_i\, |\tilde{\psi}\rangle \leqslant \epsilon$ or, equivalently, $\|P_i\,|\tilde{\psi}\rangle\| \leqslant \sqrt{\epsilon}$. Hence, given a sum-of-squares decomposition of $\overline{\mathcal{I}}_\alpha$, the action of the observables on the state is constrained for any state satisfying the self-testing criterion.

The SOS decompositions found in this article are valid for any A_x and B_y that are Hermitian and dichotomic, where A_x and B_y commute. By their definition and the assumption that Alice and Bob are separate, the physical observables $\tilde{A}_x$ and $\tilde{B}_y$ match these properties. Hence, we can derive from our two SOS decompositions some useful bounds on the action of the observables on the state.

In our SOS decompositions (A9), the P_i operators are $(2I_\alpha^{\max})^{-1/2}S_i$. We thus let $\delta = \sqrt{2I_\alpha^{\max}}\sqrt{\epsilon}$ so that the self-testing criterion implies $\|S_i\,|\tilde{\psi}\rangle\| \leqslant \delta$ for $i = 1,2,3,4$. From this, we deduce a similar bound that we will need for the action of S_5. Because $\tilde{A}_1$ is unitary and appears as a left multiplier in S_5, we can drop it from the norm $\|S_5\,|\tilde{\psi}\rangle\|$ to find the norm of a linear combination of S_2 and S_4 acting on $|\tilde{\psi}\rangle$. We then use the triangle inequality to bound this by $O(\sqrt{\epsilon})$:

$$\|S_5\,|\tilde{\psi}\rangle\| = \left\|\frac{-c}{2}S_2\,|\tilde{\psi}\rangle - \frac{\sqrt{1+s^2}}{2}S_4\,|\tilde{\psi}\rangle\right\| \tag{A12}$$

$$\leqslant \frac{c}{2}\|S_2\,|\tilde{\psi}\rangle\| + \frac{\sqrt{1+s^2}}{2}\|S_4\,|\tilde{\psi}\rangle\| \tag{A13}$$

$$\leqslant \frac{c+\sqrt{1+s^2}}{2}\delta\,. \tag{A14}$$

Now that we have $O(\delta) = O(\sqrt{\epsilon})$ bounds on $\|S_i\,|\tilde{\psi}\rangle\|$ for all i, by using the triangle inequality we can robustly certify the action of the entire subspace of operators in $\mathcal{S}_{1+AB}$ that vanish in the ideal setting, which proves to be very useful in showing the effectiveness and robustness of the self-testing isometry. Furthermore, we can extend this space beyond $\mathcal{S}_{1+AB}$ by left-multiplication by bounded operators as was done for S_5, which we will use in the self-test of measurements.

Recalling our general SOS decompositions, we notice that the four S_i polynomials in addition to the S_5 polynomial (all formulated in terms of $\tilde{A}_x$ and $\tilde{B}_y$) can be linearly combined to form the following operators, used in [6] to prove the self-test:

$$\tilde{Z}_\mathrm{A} - \tilde{Z}_\mathrm{B} = \frac{-c}{2s^2}S_1 - \frac{\sqrt{1+s^2}}{2s^2}S_3 - \frac{c}{s^2}S_5 \tag{A15}$$

$$\sin\theta\,\tilde{X}_\mathrm{A}(\mathbb{I}+\tilde{Z}_\mathrm{B}) - \cos\theta\,\tilde{X}_\mathrm{B}(\mathbb{I}-\tilde{Z}_\mathrm{A}),$$
$$= \frac{\sqrt{1+s^2}}{8\sin\theta}((c-2)S_2 + \sqrt{1+s^2}S_4)\,. \tag{A16}$$

In anticipation to the measurement self-test, we add to this list the anticommutator between Alice's two observables. This polynomial is not in $\mathcal{S}_{1+AB}$, but we can use left-multiplication to decompose it in terms of S_i:

$$\tilde{Z}_\mathrm{A}\tilde{X}_\mathrm{A} + \tilde{X}_\mathrm{A}\tilde{Z}_\mathrm{A} = \frac{\sqrt{1+s^2}}{4s^2}[-2S_2 + A_0(-cS_2 + \sqrt{1+s^2}S_4)$$
$$+ A_1(cS_1 + \sqrt{1+s^2}S_3)]\,. \tag{A17}$$

We note that the anticommutator $\{\tilde{Z}_\mathrm{B}, \tilde{X}_\mathrm{B}\}$ is 0 from definition (A3b). We will also need the following, which we write in terms of S_5 for the sake of briefness:

$$\tilde{X}_\mathrm{B} - \frac{1}{s}\tilde{X}_\mathrm{A}(\mathbb{I} - c\tilde{Z}_\mathrm{B}) = \frac{\sqrt{1+s^2}}{2s}A_1S_5\,. \tag{A18}$$

We now write down the explicit robustness bounds derived from the relations above in the same fashion as (A14):

$$\|(\tilde{Z}_\mathrm{A} - \tilde{Z}_\mathrm{B})\,|\tilde{\psi}\rangle\| \leqslant \delta_1, \tag{A19}$$

$$\|[\sin\theta\,\tilde{X}_\mathrm{A}(\mathbb{I}+\tilde{Z}_\mathrm{B}) - \cos\theta\,\tilde{X}_\mathrm{B}(\mathbb{I}-\tilde{Z}_\mathrm{A})]\,|\tilde{\psi}\rangle\| \leqslant \delta_2, \tag{A20}$$

$$\|[\tilde{X}_\mathrm{B} - s^{-1}\tilde{X}_\mathrm{A}(\mathbb{I} - c\tilde{Z}_\mathrm{B})]\,|\tilde{\psi}\rangle\| \leqslant \delta_5, \tag{A21}$$

$$\|(\tilde{Z}_\mathrm{A}\tilde{X}_\mathrm{A} + \tilde{X}_\mathrm{A}\tilde{Z}_\mathrm{A})\,|\tilde{\psi}\rangle\| \leqslant \delta_\mathrm{a}^\mathrm{A}, \tag{A22}$$

with

$$\delta_1 = (1+c)\frac{c+\sqrt{1+s^2}}{2s^2}\delta, \tag{A23}$$

$$\delta_2 = \frac{\sqrt{1+s^2}}{8\sin\theta}((2-c)+\sqrt{1+s^2})\delta, \tag{A24}$$

$$\delta_5 = \frac{\sqrt{1+s^2}(c+\sqrt{1+s^2})}{4s}\delta, \tag{A25}$$

$$\delta_\mathrm{a}^\mathrm{A} = \frac{\sqrt{1+s^2}}{2s^2}(1+c+\sqrt{1+s^2})\delta. \tag{A26}$$

We now prove that the isometry defined earlier provides a robust self-test for our reference system. This consists in applying a series of transformations on bounds (A19)–(A22) in order to reach bounds (A2). Concretely, in order to prove the self-testing bounds, the action of the unitary operators that constitute the isometry must be shown to be restricted by the self-testing criterion. If there were no need for regularization, bounds (A19)–(A22) would directly apply to the isometry. As we will show, the regularization procedure applied to define the unitaries in the isometry only introduces new error terms of the same order of $O(\sqrt{\epsilon})$ as the bounds for the unregularized operators.

a. Self-testing the state

We focus in this section on the claim of [6], that is, the self-testing bound (A2) for the state (i.e., $x = y = -1$).

We start by showing an analog of inequality (A19) for the regularized operators. To do so, we use the triangle inequality to separate $\|(Z'_\mathrm{B} - Z'_\mathrm{A})\,|\tilde{\psi}\rangle\|$ into two terms. The first one is

bounded as follows:

$$\|(Z'_{\rm B} - \tilde{Z}_{\rm B})\,|\tilde{\psi}\rangle\| = \|Z'_{\rm B}(\mathbb{I} - |\tilde{Z}_{\rm B}|)\,|\tilde{\psi}\rangle\| \quad \text{(A27)}$$
$$= \|(\mathbb{I} - |\tilde{Z}_{\rm A}\tilde{Z}_{\rm B}|)\,|\tilde{\psi}\rangle\| \quad \text{(A28)}$$
$$\leqslant \|(\mathbb{I} - \tilde{Z}_{\rm A}\tilde{Z}_{\rm B})\,|\tilde{\psi}\rangle\| \quad \text{(A29)}$$
$$\leqslant \delta_1. \quad \text{(A30)}$$

In the first equality, we used the identity $Z'_{\rm B}|\tilde{Z}_{\rm B}| = \tilde{Z}_{\rm B}$ that we highlighted when defining the regularized operators. In the second equality, we use the unitarity of $Z'_{\rm B}$ and the fact that the absolute value of an operator is unchanged by acting on the left with a unitary operator, here $\tilde{Z}_{\rm A}$. The last inequality uses the unitarity of $\tilde{Z}_{\rm A}$ again to recover (A19). Recalling that $Z'_{\rm A} = \tilde{Z}_{\rm A}$, we thus have

$$\|(Z'_{\rm B} - Z'_{\rm A})\,|\tilde{\psi}\rangle\|$$
$$\leqslant \|(Z'_{\rm B} - \tilde{Z}_{\rm B})\,|\tilde{\psi}\rangle\| + \|(\tilde{Z}_{\rm B} - Z'_{\rm A})\,|\tilde{\psi}\rangle\| \quad \text{(A31)}$$
$$\leqslant 2\delta_1. \quad \text{(A32)}$$

We then prove a bound for $X'_{\rm B}$ similar to (A30), which requires a different approach. We note that

$$\cos^2\mu\,\tilde{Z}_{\rm B}^2 + \sin^2\mu\,\tilde{X}_{\rm B}^2 = \mathbb{I}\,, \quad \text{(A33)}$$

and use it in the following chain:

$$\|(X'_{\rm B} - \tilde{X}_{\rm B})\,|\tilde{\psi}\rangle\| = \|(\mathbb{I} - |\tilde{X}_{\rm B}|)\,|\tilde{\psi}\rangle\| \quad \text{(A34)}$$
$$\leqslant \|(\mathbb{I} + |\tilde{X}_{\rm B}|)(\mathbb{I} - |\tilde{X}_{\rm B}|)\,|\tilde{\psi}\rangle\| \quad \text{(A35)}$$
$$= \cot^2(\mu)\|(\mathbb{I} - \tilde{Z}_{\rm B}^2)\,|\tilde{\psi}\rangle\| \quad \text{(A36)}$$
$$= \cot^2(\mu)\|(\mathbb{I} + \tilde{Z}_{\rm A}\tilde{Z}_{\rm B})(\mathbb{I} - \tilde{Z}_{\rm A}\tilde{Z}_{\rm B})\,|\tilde{\psi}\rangle\| \quad \text{(A37)}$$
$$\leqslant \cot^2(\mu)(1 + (\cos\mu)^{-1})\delta_1 \equiv \delta_4. \quad \text{(A38)}$$

The first equality uses unitarity and the property $X'_{\rm B}|\tilde{X}_{\rm B}|=\tilde{X}_{\rm B}$. The first inequality uses the operator inequality $\mathbb{I} + |\tilde{X}_{\rm B}| \succeq \mathbb{I}$. The second equality uses (A33). The last inequality uses (A33) again to put a bound on $\|\tilde{Z}_{\rm B}\|_\infty$.

We now turn to the self-testing statement. In the isometry output (A4), because $Z'_{\rm A}$ and $Z'_{\rm B}$ have near-identical action over the state by bound (A32), the dichotomicity of the regularized operators makes the two middle terms approximately vanish. In the first and last terms, for the same reason, the projectors $(\mathbb{I} \pm Z'_{\rm A})/2$ and $(\mathbb{I} \pm Z'_{\rm B})/2$ are nearly identical, and idempotence can be used. In the first term, the error introduced by this approximation is bounded as follows:

$$\left\|\left(\frac{\mathbb{I}+Z'_{\rm A}}{2}\frac{\mathbb{I}+Z'_{\rm B}}{2} - \frac{\mathbb{I}+Z'_{\rm A}}{2}\right)|\tilde{\psi}\rangle\right\|$$
$$= \frac{1}{4}\|(\mathbb{I}+Z'_{\rm A})((\mathbb{I}+Z'_{\rm B}) - (\mathbb{I}+Z'_{\rm A}))\,|\tilde{\psi}\rangle\| \quad \text{(A39)}$$
$$\leqslant \frac{1}{2}\|Z'_{\rm B} - Z'_{\rm A}\| \leqslant \delta_1. \quad \text{(A40)}$$

We used the fact that $(\mathbb{I}+Z'_{\rm A})^2 = 2(\mathbb{I}+Z'_{\rm A})$ in the first equality, and the operator bound $\|\mathbb{I}+Z'_{\rm A}\|_\infty \leqslant 2$ in the first inequality. By the same reasoning, and using the fact that $X'_{\rm A}$ and $X'_{\rm B}$ are unitary to discard them from the norm, the fourth term leads to the same bound:

$$\left\|X'_{\rm A}X'_{\rm B}\left(\frac{\mathbb{I}-Z'_{\rm A}}{2}\frac{\mathbb{I}-Z'_{\rm B}}{2} - \frac{\mathbb{I}-Z'_{\rm A}}{2}\right)|\tilde{\psi}\rangle\right\| \leqslant \delta_1\,. \quad \text{(A41)}$$

The two middle terms are similarly bounded using the orthogonality of complementary projectors:

$$\left\|\frac{\mathbb{I}\mp Z'_{\rm A}}{2}\frac{\mathbb{I}\pm Z'_{\rm B}}{2}\,|\tilde{\psi}\rangle - 0\right\|$$
$$\leqslant \frac{1}{4}\|(\mathbb{I}\mp Z'_{\rm A})((\mathbb{I}\pm Z'_{\rm B}) - (\mathbb{I}\pm Z'_{\rm A}))\,|\tilde{\psi}\rangle\| \quad \text{(A42)}$$
$$\leqslant \delta_1. \quad \text{(A43)}$$

Putting these bounds together, we deduce that replacing the isometry output with the state

$$\frac{\mathbb{I}+Z'_{\rm A}}{2}\,|\tilde{\psi}\rangle\,|00\rangle + X'_{\rm A}X'_{\rm B}\frac{\mathbb{I}-Z'_{\rm A}}{2}\,|\tilde{\psi}\rangle\,|11\rangle \quad \text{(A44)}$$

yields error terms bounded by $4\delta_1$. We note that this state is only approximately normalized.

We now take this approximation further to show that, as in the ideal case, the physical registers in the two terms are (approximately) proportional to the same state, which we call $|\text{junk}\rangle$ and define as

$$|\text{junk}\rangle = \beta^{-1}\frac{\mathbb{I}+Z'_{\rm A}}{2\cos\theta}\,|\tilde{\psi}\rangle\,, \quad \text{(A45)}$$

where $\beta \geqslant 0$ is such that $\||\text{junk}\rangle\| = 1$. We will later show that $\beta \simeq 1$. The first term in (A44) is therefore $\beta\cos\theta\,|\text{junk}\rangle\,|00\rangle$. We show proportionality for the second term:

$$\left\|X'_{\rm A}X'_{\rm B}\frac{\mathbb{I}-Z'_{\rm A}}{2}\,|\tilde{\psi}\rangle - \beta\sin\theta\,|\text{junk}\rangle\right\|$$
$$= \left\|\left(X'_{\rm A}X'_{\rm B}\frac{\mathbb{I}-Z'_{\rm A}}{2} - \tan\theta\frac{\mathbb{I}+Z'_{\rm A}}{2}\right)|\tilde{\psi}\rangle\right\| \quad \text{(A46)}$$
$$\leqslant \left\|\left(X'_{\rm B}\frac{\mathbb{I}-Z'_{\rm A}}{2} - X'_{\rm A}\tan\theta\frac{\mathbb{I}+Z'_{\rm B}}{2}\right)|\tilde{\psi}\rangle\right\|$$
$$+ \left\|\tan\theta\left(\frac{Z'_{\rm B}-Z'_{\rm A}}{2}\right)|\tilde{\psi}\rangle\right\|. \quad \text{(A47)}$$

The first equality uses the definition of $|\text{junk}\rangle$. The inequality uses the triangle inequality and the unitarity of $X'_{\rm A}$ on the first term. The second term can be bounded by (A32). We can see that the first term is similar to bound (A20), from which we now derive an equivalent for the regularized operators:

$$\|(\cos\theta X'_{\rm B}(\mathbb{I} - Z'_{\rm A}) - \sin\theta X'_{\rm A}(\mathbb{I} + Z'_{\rm B}))\,|\tilde{\psi}\rangle\|$$
$$\leqslant \|(\cos\theta\tilde{X}_{\rm B}(\mathbb{I} - \tilde{Z}_{\rm A}) - \tilde{X}_{\rm A}\sin\theta(\mathbb{I} + \tilde{Z}_{\rm B}))\,|\tilde{\psi}\rangle\|$$
$$+\|\cos\theta(\mathbb{I} - Z'_{\rm A})(X'_{\rm B} - \tilde{X}_{\rm B})\,|\tilde{\psi}\rangle\|$$
$$+\|\sin\theta X'_{\rm A}(\tilde{Z}_{\rm B} - Z'_{\rm B})\,|\tilde{\psi}\rangle\| \quad \text{(A48)}$$
$$\leqslant \delta_2 + 2\delta_4\cos\theta + \delta_1\sin\theta \equiv \delta'_2. \quad \text{(A49)}$$

The first inequality uses two triangle inequalities, the identities $Z'_{\rm A} = \tilde{Z}_{\rm A}$ and $X'_{\rm A} = \tilde{X}_{\rm A}$ and the commutation of these operators with Bob's.

All in all, (A47) is thus bounded by $\tan\theta\delta_1 + \delta'_2/\cos\theta$, and we end up with the following bound showing an approximate

tensor product structure on the output state:

$$\|\Phi(|\tilde{\psi}\rangle) - \beta\,|\text{junk}\rangle\,|\psi\rangle\| \leqslant (4+\tan\theta)\delta_1 + \frac{\delta_2'}{2\cos\theta} \equiv \bar{\delta}\,. \tag{A50}$$

The last error term to recover the state self-testing statement (A2) is to show that $\beta \simeq 1$. To do so, we bound $1-\beta$ from above and below. First, using the property that the isometry preserves the norm, we find

$$1 = \|\Phi(|\tilde{\psi}\rangle)\| \tag{A51}$$

$$\leqslant \|\Phi(|\tilde{\psi}\rangle) - \beta\,|\text{junk}\rangle\,|\psi\rangle\| + \beta\|\,|\text{junk}\rangle\,|\psi\rangle\| \tag{A52}$$

$$\leqslant \bar{\delta} + \beta. \tag{A53}$$

Similarly, we have

$$\beta = \|\beta\,|\text{junk}\rangle\,|\psi\rangle\| \tag{A54}$$

$$\leqslant \|\beta\,|\text{junk}\rangle\,|\psi\rangle - \Phi(|\tilde{\psi}\rangle)\| + \|\Phi(|\tilde{\psi}\rangle)\| \tag{A55}$$

$$\leqslant \bar{\delta} + 1. \tag{A56}$$

Put together, β is constrained as $|1-\beta| \leqslant \bar{\delta}$. Using this and (A50), we finally complete the proof for the self-testing statement on the state

$$\|\Phi(|\tilde{\psi}\rangle) - |\text{junk}\rangle\,|\psi\rangle\| \leqslant 2\bar{\delta}\,. \tag{A57}$$

b. Self-testing the measurements

The proof for the self-testing statements involving operator actions in (A2) builds on the previous section. As a first step, we give approximations on the output of the isometry when acting on the input with the *regularized* operators, and then further approximate by substituting them with the nonregularized operators.

This is where we need the approximate anticommutation of $X_{\rm A}'$ and $Z_{\rm A}'$ when acting on the state, given by inequality (A22). We will also need to prove a similar anticommutation bound for $X_{\rm B}'$ and $Z_{\rm B}'$. As we noted earlier, the nonregularized $\tilde{X}_{\rm B}$ and $\tilde{Z}_{\rm B}$ anticommute by definition, but the regularization procedure breaks this. As a result, we can only prove that $\{\tilde{X}_{\rm B},\tilde{Z}_{\rm B}\}\,|\tilde{\psi}\rangle \simeq 0$, which will require a number of successive approximations.

The use of anticommutation is made clear when looking at the action of the isometry (A4) on $X_{\rm A}'\,|\tilde{\psi}\rangle$ or $X_{\rm B}'\,|\tilde{\psi}\rangle$. For example (the reasoning for the other operator is the same),

$$\begin{aligned}\Phi(X_{\rm A}'\,|\tilde{\psi}\rangle) =& \tfrac{1}{4}[(\mathbb{I}+Z_{\rm B}')(\mathbb{I}-X_{\rm A}'Z_{\rm A}'X_{\rm A}')\,|\tilde{\psi}\rangle\,|10\rangle \\ &+ X_{\rm A}'(\mathbb{I}+Z_{\rm B}')(\mathbb{I}+X_{\rm A}'Z_{\rm A}'X_{\rm A}')\,|\tilde{\psi}\rangle\,|00\rangle \\ &+ X_{\rm B}'(\mathbb{I}-Z_{\rm B}')(\mathbb{I}-X_{\rm A}'Z_{\rm A}'X_{\rm A}')\,|\tilde{\psi}\rangle\,|11\rangle \\ &+ X_{\rm A}'X_{\rm B}'(\mathbb{I}-Z_{\rm B}')(\mathbb{I}+X_{\rm A}'Z_{\rm A}'X_{\rm A}')\,|\tilde{\psi}\rangle\,|01\rangle]\,.\end{aligned} \tag{A58}$$

The approximate anticommutation of $X_{\rm A}'$ and $Z_{\rm A}'$ means that $X_{\rm A}'Z_{\rm A}'X_{\rm A}'\,|\tilde{\psi}\rangle \simeq -Z_{\rm A}'\,|\tilde{\psi}\rangle$, and this output only differs from $\Phi(|\tilde{\psi}\rangle)$ by the action of σ_x on the first ancilla qubit, and a small error term. On the other hand, it is easily seen that the isometry applied on $Z_{\rm A}'\,|\tilde{\psi}\rangle$ or $Z_{\rm B}'\,|\tilde{\psi}\rangle$ yields exactly the output $\Phi(|\tilde{\psi}\rangle)$ with the σ_z Pauli operator acting on the corresponding ancilla.

We now prove the anticommutation bound for Bob's operators. Compared to the other bounds we have derived so far, this is not as immediate as it might seem; indeed, while we know by (A30) and (A38) that the nonregularized and regularized X and Z operators on Bob's side are approximately interchangeable, this is only the case when they act on the physical state $|\tilde{\psi}\rangle$. Thus, we cannot deduce from this alone that $\{X_{\rm B}',Z_{\rm B}'\}\,|\tilde{\psi}\rangle \simeq \{\tilde{X}_{\rm B},\tilde{Z}_{\rm B}\}\,|\tilde{\psi}\rangle = 0$ because not all unitaries in the anticommutator act directly on the state. Instead, what we do is to approximate the rightmost operator in each term of the anticommutator by its unnormalized counterpart by using (A30) and (A38), and translate the action of $\tilde{Z}_{\rm B}$ and $\tilde{X}_{\rm B}$ into one that commutes with the leftmost operators using respectively (A19) and (A21). Then, the leftmost operators can in turn be approximated because they now act on the state directly.

The steps outlined above are carried out as follows:

$$\|\{X_{\rm B}',Z_{\rm B}'\}\,|\tilde{\psi}\rangle\|$$

$$\leqslant 2\delta_1 + \|(\tilde{Z}_{\rm A}+Z_{\rm B}')X_{\rm B}'\,|\tilde{\psi}\rangle\| \tag{A59}$$

$$\leqslant 2\delta_1 + 2\delta_4 + 2\delta_5 + s^{-1}\|(\tilde{Z}_{\rm A}+Z_{\rm B}')\tilde{X}_{\rm A}(\mathbb{I}-c\tilde{Z}_{\rm B})\,|\tilde{\psi}\rangle\| \tag{A60}$$

$$= 2\delta_1 + 2\delta_4 + 2\delta_5 + s^{-1}\|(\mathbb{I}-c\tilde{Z}_{\rm B})(\tilde{Z}_{\rm A}+Z_{\rm B}')\tilde{X}_{\rm A}\,|\tilde{\psi}\rangle\| \tag{A61}$$

$$\leqslant 2\delta_1 + 2\delta_4 + 2\delta_5 + \frac{1+c/\cos\mu}{s}\|\tilde{Z}_{\rm A}\tilde{X}_{\rm A} + \tilde{X}_{\rm A}Z_{\rm B}'\,|\tilde{\psi}\rangle\| \tag{A62}$$

$$\leqslant 2\delta_1 + 2\delta_4 + 2\delta_5 + \frac{1+c/\cos\mu}{s}\left(2\delta_1 + \delta_{\rm a}^{\rm A}\right) \tag{A63}$$

$$\equiv \delta_{\rm a}^{\rm B}. \tag{A64}$$

In the first inequality, we used (A32). The second inequality uses (A38) followed by (A21), which lets us commute this approximation of $X_{\rm B}'$ to the left of the operator product in the first equality. Next, in the third inequality, the operator bound $\|\tilde{Z}_{\rm B}\|_\infty \leqslant (\cos\mu)^{-1}$ that we used to derive (A38) is used again. Finally, we use (A32) followed by Alice's anticommutation bound (A22) to reach the last inequality.

Thus, combining the anticommutation bounds with the regularization approximations for Bob's operators (A30) and (A38), we find

$$\|\Phi(\tilde{Z}_{\rm A}\,|\tilde{\psi}\rangle) - \sigma_z^{\rm A}\Phi(|\tilde{\psi}\rangle)\| = 0, \tag{A65}$$

$$\|\Phi(\tilde{X}_{\rm A}\,|\tilde{\psi}\rangle) - \sigma_x^{\rm A}\Phi(|\tilde{\psi}\rangle)\| \leqslant 2\delta_{\rm a}^{\rm A}, \tag{A66}$$

$$\|\Phi(\tilde{Z}_{\rm B}\,|\tilde{\psi}\rangle) - \sigma_z^{\rm B}\Phi(|\tilde{\psi}\rangle)\| \leqslant \delta_1, \tag{A67}$$

$$\|\Phi(\tilde{X}_{\rm B}\,|\tilde{\psi}\rangle) - \sigma_x^{\rm B}\Phi(|\tilde{\psi}\rangle)\| \leqslant \delta_4 + 2\delta_{\rm a}^{\rm B}. \tag{A68}$$

In the last two bounds, we have also used the fact that Φ preserves the norms and is linear, such that for example $\|\Phi(\tilde{Z}_{\rm B}\,|\tilde{\psi}\rangle) - \Phi(Z_{\rm B}'\,|\tilde{\psi}\rangle)\| = \|(\tilde{Z}_{\rm B} - Z_{\rm B}')\,|\tilde{\psi}\rangle\|$.

Our goal is to reach bounds from the joint action of the observables $\tilde{A}_x$ and $\tilde{B}_y$. So far, we can only compute bounds for the action of one party at a time. Indeed, to bound $\|\Phi(\tilde{B}_y\,|\tilde{\psi}\rangle) - B_y\Phi(|\tilde{\psi}\rangle)\|$ we can use definition (A1a) for B_y, the triangle inequality, and the bounds above for the action of $\tilde{Z}_{\rm B}$ and $\tilde{X}_{\rm B}$.

We now show that with joint action of both parties, Alice's operator is easily dealt with. First, consider $\Phi(\tilde{A}_0\tilde{B}_y\,|\tilde{\psi}\rangle)$. As with (A65), this is exactly the same as $A_0\Phi(\tilde{B}_y\,|\tilde{\psi}\rangle)$

because $\tilde{A}_0 = Z'_{\mathrm{A}}$ and $A_0 = \sigma_z^{\mathrm{A}}$. Next is $\Phi(\tilde{A}_1 \tilde{B}_y |\tilde{\psi}\rangle)$, for which it is easily seen that the reasoning that we used to reach (A66) is unchanged. Indeed $A_1 = X'_{\mathrm{A}}$, and this state is identical to (A58) with $|\tilde{\psi}\rangle$ replaced with $\tilde{B}_y |\tilde{\psi}\rangle$. We use commutation between Alice and Bob to move $\tilde{B}_y$ to the left of $(\mathbb{I} \pm X'_{\mathrm{A}} Z'_{\mathrm{A}} X'_{\mathrm{A}})$ and, because $\|\tilde{B}_y\|_\infty = 1$, we find

$$\|\Phi(\tilde{A}_1 \tilde{B}_y |\tilde{\psi}\rangle) - A_1 \Phi(\tilde{B}_y |\tilde{\psi}\rangle)\| \leqslant 2\delta_{\mathrm{a}}^{\mathrm{A}} . \tag{A69}$$

We have thus showed that (A65) and (A66) are unchanged if we replace $|\tilde{\psi}\rangle$ with $\tilde{B}_y |\tilde{\psi}\rangle$ in both terms.

In addition to the above, we will use one last approximation to replace the isometry output $\Phi(|\tilde{\psi}\rangle)$ with $|\mathrm{junk}\rangle |\psi\rangle$, at the cost of the additional error term of $2\bar{\delta}$ from (A57). We finally find the following bounds $e_{xy}(\epsilon)$ in the self-testing statement (A2), where we define $e_{xy} = e'_{xy} + 2\bar{\delta}$:

$$e'_{-1,-1} = e'_{0,-1} = 0 , \tag{A70}$$

$$e'_{1,-1} = 2\delta_{\mathrm{a}}^{\mathrm{A}} , \tag{A71}$$

$$\begin{aligned} e'_{-1,0} &= e'_{-1,1} = e'_{0,0} = e'_{0,1} \\ &= \delta_1 \cos\mu + (\delta_4 + 2\delta_{\mathrm{a}}^{\mathrm{B}}) \sin\mu , \end{aligned} \tag{A72}$$

$$e'_{1,0} = e'_{1,1} = 2\delta_{\mathrm{a}}^{\mathrm{A}} + e'_{-1,0} . \tag{A73}$$

APPENDIX B: ADDITIONAL SOS FOR CHSH

By guessing values for the parameters in (14), other nontrivial SOS decompositions than (17) and (18) can be found.

We report here a combination that leads to a SOS matrix of rank 4 which is extremal in the set represented in Fig. 3, i.e., it cannot be decomposed as a convex combination of SOS matrices of the same form as (14). With the values $q = 1/4$, $\mu = 5/8, \lambda = 1/4$, the square root of M is rather well-behaved, and leads to the following SOS decomposition:

$$\begin{aligned} \overline{\mathcal{I}}_0 = \frac{1}{8\sqrt{2}} [&2(Z_{\mathrm{A}} - Z_{\mathrm{B}})^2 + 5(X_{\mathrm{A}} - X_{\mathrm{B}})^2 \\ &+ 2(Z_{\mathrm{A}} X_{\mathrm{B}} + X_{\mathrm{A}} Z_{\mathrm{B}})^2 \\ &+ (3 - 2Z_{\mathrm{A}} Z_{\mathrm{B}} - X_{\mathrm{A}} X_{\mathrm{B}})^2] . \end{aligned} \tag{B1}$$

An additional symmetry of the CHSH inequality can be exploited to reach an additional SOS decomposition: swapping X and Z (i.e., swapping the observables A_0 and A_1 and changing B_1 to $-B_1$) leaves $\overline{\mathcal{I}}_0$ invariant, and therefore

$$\begin{aligned} \overline{\mathcal{I}}_0 = \frac{1}{8\sqrt{2}} [&2(X_{\mathrm{A}} - X_{\mathrm{B}})^2 + 5(Z_{\mathrm{A}} - Z_{\mathrm{B}})^2 \\ &+ 2(Z_{\mathrm{A}} X_{\mathrm{B}} + X_{\mathrm{A}} Z_{\mathrm{B}})^2 \\ &+ (3 - 2X_{\mathrm{A}} X_{\mathrm{B}} - Z_{\mathrm{A}} Z_{\mathrm{B}})^2] , \end{aligned} \tag{B2}$$

for which the parameter values are q=1/4, μ=1/4, λ=5/8.

It is not clear whether either of these decompositions yields an easy generalization to the whole $\overline{\mathcal{I}}_\alpha$ family.

APPENDIX C: SHORTCOMINGS IN PREVIOUS RESULTS

1. CHSH self-test

In their robust self-test proof for the maximal CHSH violation, McKague *et al.* [11] introduce the isometry used in [6] and in the present article, with the same regularization construct we used on operators (A3) to build the unitaries that make up the isometry. The proof technique is the same as in this article: they identify from the self-testing criterion a series of constraints on the action of the observables in the system, that are then combined to form the self-testing statement. However, in their self-test of the observables, the authors rely on the anticommutation relation $\{X'_{\mathrm{B}}, Z'_{\mathrm{B}}\} = 0$ on Bob's regularized operators. As we noted, although $\tilde{X}_{\mathrm{B}}$ and $\tilde{Z}_{\mathrm{B}}$ (in our notation) anticommute by definition, this property is lost to regularization. Indeed, the nonzero eigenvalues of anticommuting operators come in pairs of opposite sign, which means that nonsingular anticommuting operators do not exist in odd-dimensional Hilbert spaces. In fact, if B_0 and B_1 do not each have as many $+1$ as -1 eigenvalues, their eigenspaces must share a nontrivial intersection, which will be an eigenspace for both X'_{B} and Z'_{B} (with nonzero eigenvalue because of regularization) where these two operators can therefore not anticommute. Hence, in their proof in Appendix B of [11], while $B'_0 \pm B'_1$ anticommute, it is not true anymore when their zero eigenvalues are replaced with 1.

However, this oversight only affects the final result by error terms of the same robustness order as they claim. Indeed, as they show in the proof for their second self-testing criterion based on Mayers and Yao's work, the anticommutation of X'_{B} and Z'_{B} in front of the physical state $|\psi'\rangle$ can still be given a robustness bound. This follows from the $O(\sqrt{\epsilon})$ bound on the anticommutation of Alice's X'_{A} and Z'_{A} operators and the $O(\epsilon^{1/4})$ bounds on the replacement of Bob's X' and Z' operators by Alice's, which can be combined to transform Alice's anticommutation bound to one for Bob with $O(\epsilon^{1/4})$ order. Although this is worse than the $\epsilon_2 \in O(\sqrt{\epsilon})$ that they use in their Theorem 1, the final order in the self-testing bounds is unchanged by this correction because they already contain $O(\epsilon^{1/4})$ terms from Alice's anticommutation bound.

2. Partially entangled state self-test

In their proof for the self-test statement (A2) on the state (i.e., $x = y = -1$), Yang and Navascués introduce a SOS decomposition for $\overline{\mathcal{I}}_\alpha$ different from ours [6]. They write the SOS polynomials P_i as products $\mathbf{q}_i \cdot \mathbf{V}$ with $\mathbf{V}$ defined as in (9), and $\mathbf{q}_i$ decomposed in terms of five nine-dimensional vectors $\mathbf{r}_i$ different from the ones we defined in (13). We reproduce here the q_i they list in their article, with a change in q_2 which originally contained a typo that was communicated to us [15]:

$$\mathbf{q}_1 = \frac{\gamma}{20\sqrt{2}} (\mathbf{r}_5 - \mathbf{r}_4) - \frac{2}{5} \mathbf{r}_1 , \tag{C1}$$

$$\mathbf{q}_2 = \frac{\sqrt{25\sqrt{1+s^2} - 9 - \gamma^2/8}}{10s} (\mathbf{r}_1 + c\mathbf{r}_2 - c\mathbf{r}_3) \tag{C2}$$

$$\mathbf{q}_3 = \frac{2\gamma - 25c\sqrt{3-\bar{c}}}{30\sqrt{2}} \mathbf{r}_1 + \frac{3}{10} (\mathbf{r}_5 - \mathbf{r}_4) , \tag{C3}$$

$$\mathbf{q}_4 = \frac{35}{100} (\mathbf{r}_3 + \mathbf{r}_2) - \frac{5c\sqrt{3-\bar{c}}}{14\sqrt{2}} \mathbf{r}_1 , \tag{C4}$$

$$\mathbf{q}_5 = \frac{\sqrt{49\gamma^2 + 9800c\gamma\sqrt{3-\bar{c}} + \omega}}{420} \mathbf{r}_1 , \tag{C5}$$

with $\bar{c} = \cos(4\theta)$; $\gamma = \sqrt{(75+25\bar{c})\sqrt{6-2\bar{c}}-72}$; and $\omega = 18\,125\cos(8\theta) - 72\,500\cos(4\theta) - 108\,706$. Their SOS is then defined as

$$\overline{\mathcal{I}}_\alpha = \sum_{i=1}^{5} (\mathbf{q}_i \cdot \mathbf{V})^\dagger (\mathbf{q}_i \cdot \mathbf{V}). \tag{C6}$$

This decomposition is problematic. Indeed, the vector $\mathbf{q}_5$ is real only in the interval in θ (or equivalently in α) where the expression inside the square root in (C5) is positive. This corresponds approximately to $\theta \in [0.075\,74, 0.730\,14]$, which is not the full interval $]0,\pi/4] =]0, 0.785\,40]$. Outside of that interval, a change of sign of the fifth term in (C6) is actually required to recover the left-hand side. However, this change means that the decomposition of $\overline{\mathcal{I}}_\alpha$, while valid, is not a sum of squares anymore, and therefore it does not have the properties required for the self-test proof. The value $\theta = \pi/8$ is within the validity interval; we represent the SOS in Fig. 2 as a red dot.

Another issue with this decomposition is that the $\mathbf{q}_i$ vectors have a linear dependency that went unnoticed in the original article. This can be seen in the fact that all five $\mathbf{q}_i$ only depend on $\mathbf{r}_4$ and $\mathbf{r}_5$ through their difference $\mathbf{r}_5 - \mathbf{r}_4$, which means that the $\mathbf{q}_i$ only span a four-dimensional subspace. Hence, this is insufficient to certify the five operator identities in $\mathcal{S}_{1+AB}$. Notably, forming the operator on the left hand side of (A16) in the present article from their polynomials $\mathbf{q}_i \cdot \mathbf{V}$ requires a decomposition of $\mathbf{r}_5 + \mathbf{r}_4$ in terms of the $\mathbf{q}_i$ vectors as noted in the supplemental information to their article, which is not possible.

The linear dependency between the $\mathbf{q}_i$ is also visible in Fig. 2. Indeed, the points on the boundary of this set correspond to singular SOS matrices M, as the nonsingular matrices, being strictly positive definite, do not saturate the inequalities that define the boundary. Therefore, for this SOS decomposition, M is singular (i.e., of rank at most 4 here) and the $\mathbf{q}_i$ can therefore not be linearly independent.

TABLE I. Vertex SOS decompositions for CHSH.

C₁ $\lambda = 0, \mu = 0, q = 0$

$$M = \frac{1}{2\sqrt{2}}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{C7}$$

$$\overline{\mathcal{I}}_0 = \frac{1}{2\sqrt{2}}\left[R_2^2 + R_3^2\right] = \frac{1}{\sqrt{2}}[(-\mathbb{I} + Z_\mathrm{A}Z_\mathrm{B})^2 + (-\mathbb{I} + X_\mathrm{A}X_\mathrm{B})^2]; \tag{C8}$$

C₂ $\lambda = 1, \mu = 0, q = 0$

$$M = \frac{1}{2\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{C9}$$

$$\overline{\mathcal{I}}_0 = \frac{1}{2\sqrt{2}}\left[R_1^2 + R_3^2\right] = \frac{1}{\sqrt{2}}[(-Z_\mathrm{A} + Z_\mathrm{B})^2 + (-\mathbb{I} + X_\mathrm{A}X_\mathrm{B})^2]; \tag{C10}$$

C₃ $\lambda = 0, \mu = 1, q = 0$

$$M = \frac{1}{2\sqrt{2}}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{C11}$$

$$\overline{\mathcal{I}}_0 = \frac{1}{2\sqrt{2}}\left[R_2^2 + R_4^2\right] = \frac{1}{\sqrt{2}}[(-\mathbb{I} + Z_\mathrm{A}Z_\mathrm{B})^2 + (-X_\mathrm{A} + X_\mathrm{B})^2]; \tag{C12}$$

C₄ $\lambda = 1, \mu = 1, q = 0,$

$$M = \frac{1}{2\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{C13}$$

$$\overline{\mathcal{I}}_0 = \frac{1}{2\sqrt{2}}\left[R_1^2 + R_4^2\right] = \frac{1}{\sqrt{2}}[(-Z_\mathrm{A} + Z_\mathrm{B})^2 + (-X_\mathrm{A} + X_\mathrm{B})^2]; \tag{C14}$$

C₅ $\lambda = 0, \mu = 0, q = 1/2$

$$M = \frac{1}{2\sqrt{2}}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 \end{pmatrix}, \tag{C15}$$

$$\begin{aligned}\overline{\mathcal{I}}_0 &= \frac{1}{4\sqrt{2}}\left[(R_2 + R_3)^2 + R_5^2\right] \\ &= \frac{1}{4\sqrt{2}}[(-2\sqrt{2}\,\mathbb{I} + \overline{\mathcal{I}}_0)^2 + 2(Z_\mathrm{A}X_\mathrm{B} + X_\mathrm{A}Z_\mathrm{B})^2] = \frac{1}{4\sqrt{2}}\left[\overline{\mathcal{I}}_0^2 + \mathcal{S}'^2\right],\end{aligned} \tag{C16}$$

where $\mathcal{S}' = A_0(B_0 - B_1) + A_1(B_0 + B_1)$.

[1] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[2] A. Acín, S. Massar, and S. Pironio, Randomness versus nonlocality and entanglement, Phys. Rev. Lett. **108**, 100402 (2012).

[3] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner, The Quantum moment problem and bounds on entangled multi-prover games, in *23rd Annual IEEE Conference on Computational Complexity, 2008, CCC'08* (Los Alamitos, CA, USA, 2008), pp. 199–210.

[4] M. Navascués, S. Pironio, and A. Acín, Bounding the set of quantum correlations, Phys. Rev. Lett. **98**, 010401 (2007).

[5] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys. **10**, 073013 (2008).

[6] T. H. Yang and M. Navascués, Robust self-testing of unknown quantum systems into any entangled two-qubit states, Phys. Rev. A **87**, 050102 (2013).

[7] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inf. Comput. **4**, 273 (2004).

[8] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, Nature (London) **496**, 456 (2013).

[9] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, arXiv:1402.0489 [quant-ph] (2014).

[10] M. L. Almeida, J.-D. Bancal, N. Brunner, A. Acín, N. Gisin, and S. Pironio, Guess your neighbor's input: A multipartite nonlocal game with no quantum advantage, Phys. Rev. Lett. **104**, 230404 (2010).

[11] M. McKague, T. H. Yang, and V. Scarani, Robust self-testing of the singlet, J. Phys. A: Math. Theor. **45**, 455304 (2012).

[12] J. Sturm, Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones, Optim. Methods Software **11–12**, 625 (1999); version 1.05 available from http://fewcal.kub.nl/sturm.

[13] K. Gatermann and P. A. Parrilo, Symmetry groups, semidefinite programs, and sums of squares, J. Pure Appl. Algebra **192**, 95 (2004).

[14] R. Bhatia, *Positive Definite Matrices* (Princeton University Press, Princeton, 2009).

[15] T. H. Yang (private communication, 2014).