Proofs of the Kochen-Specker theorem based on the N-qubit Pauli group

Mordecai Waegell* and P. K. Aravind†
Physics Department, Worcester Polytechnic Institute, Worcester, Massachusetts 01609, USA
(Received 19 March 2013; published 1 July 2013)

We present a number of observables-based proofs of the Kochen-Specker (KS) theorem based on the N-qubit Pauli group for $N \geqslant 4$, thus adding to the proofs that have been presented earlier for the 2- and 3-qubit groups. These proofs have the attractive feature that they can be presented in the form of diagrams from which they are obvious by inspection. They are also irreducible in the sense that they cannot be reduced to smaller proofs by ignoring some subset of qubits and/or observables in them. A simple algorithm is given for transforming any observables-based KS proof into a large number of projectors-based KS proofs; if the observables-based proof has O observables, with each observable occurring in exactly two commuting sets and any two commuting sets having at most one observable in common, the number of associated projectors-based parity proofs is 2^O. We introduce symbols for the observables- and projectors-based KS proofs that capture their important features and also convey a feeling for the enormous variety of both these types of proofs within the N-qubit Pauli group. We discuss an infinite family of observables-based proofs, whose members include all numbers of qubits from 2 up, and show how it can be used to generate projectors-based KS proofs involving only 9 bases (or experimental contexts) in any dimension of the form 2^N for $N \geqslant 2$. Some implications of our results are discussed.

DOI: 10.1103/PhysRevA.88.012102 PACS number(s): 03.65.Ud, 03.65.Aa, 03.67.−a

I. INTRODUCTION

In a recent paper [1] we pointed out that the N-qubit Pauli group (for $N \geqslant 2$) is a rich source of both observables-based and projectors-based "parity proofs" of the Kochen-Specker (KS) theorem [2]. We refer to the proofs as parity proofs because, in either the observables-based version or the projectors-based version, they exploit the concept of parity to achieve their ends. The purpose of this paper is to give examples of both types of proofs for 4- and higher qubit systems and to point out several of their properties that we did not discuss earlier in our work on 2- and 3-qubit systems [3,4]. More precisely, the goals of this paper are the following:

(1) We explain what we mean by an observables-based KS proof and show how it can be depicted in the form of a diagram from which it is obvious by inspection. The two best-known examples of such proofs are a 2-qubit proof due to Peres [5] and Mermin [6] and a 3-qubit proof due to Mermin [6] based on earlier work by Greenberger, Horne, and Zeilinger [7]. In Ref. [4] we presented several examples of 2- and 3-qubit proofs of this kind and in Ref. [1] we indicated that we had found a large number of 4- and higher qubit proofs but gave few details. Here we give examples of 4-, 5-, and 6-qubit proofs that convey a feeling for the wide variety of possibilities that open up as one goes to a larger number of qubits. We should stress that we consider only *critical* proofs, i.e., ones that cannot be reduced to smaller proofs by omitting some subset of qubits and/or observables in them, but that despite this restriction the number of possibilities still grows very rapidly as one goes to a larger number of qubits.

(2) We show how any observables-based KS proof can be used to construct a system of projectors and bases from which a large number of projectors-based parity proofs of the KS theorem can be obtained. The simplest example of this procedure is provided by the 2-qubit Peres-Mermin square, whose 9 observables give rise to a system of projectors and bases that yield a total of $2^9 = 512$ projectors-based parity proofs [8–11]. In recent years a number of other examples of projectors-based parity proofs have been found in four [3,12] and eight [4,13] dimensions. A major point of this paper is that every observables-based parity proof, based on a subset of observables of the Pauli group, gives rise to a system of projectors-based parity proofs, and we give a simple algorithm for making this transition. We illustrate this algorithm in the particular case of a 4-qubit observables-based proof and show how the 2^{12} associated projectors-based proofs can be obtained with practically no effort (once the system of projectors and bases within which they are embedded has been set up). In addition to the fact that they are easy to generate, the projectors-based proofs are also easy to check, since only simple counting is called for. Like the observables-based proofs from which they are derived, the projectors-based proofs are critical in the sense that they cannot be whittled down to smaller proofs by omitting some subset of their bases. Because each observables-based proof gives rise to a large number of projectors-based proofs, the variety and quantity of the latter are vastly greater than those of the former.

(3) It is interesting to ask if there are any infinite classes of observables-based proofs that apply to all numbers of qubits from 2 up. We have discovered several such classes that we call the star class, the wheel class, the whorl class, and the kite class (with the names reflecting the shapes of the associated diagrams). The most complex of these families is the kite class, and we give a detailed discussion of it in this paper. All the members of this family can be represented by diagrams having the form of a kite, with the body consisting of 9 observables arranged on a 3×3 grid and the tail consisting of a string of observables of arbitrary length. For any number of qubits, a suitable choice of observables (and often more than one) can be placed on the framework of a diagram of the kite class to yield a KS proof. The 2-qubit Peres-Mermin square can be regarded as a kite diagram without a tail, and the higher qubit

*caiw@wpi.edu
†paravind@wpi.edu

proofs of this family involve tails of increasing lengths. An interesting feature of this family is that all its members give rise to projectors-based KS proofs involving just 9 bases (or experimental contexts)and so are the most compact proofs of this type known in 2^N dimensions for all $N \geqslant 2$.

The next three sections are devoted to a discussion of the above three points. We then comment on the significance of our results and their relation to other work. Although this paper builds upon our earlier work [1,3,4], it is written to be self-contained and requires no familiarity with that work.

II. OBSERVABLES-BASED KS PROOFS

An observables-based proof of the KS theorem for a system of N qubits consists of a subset of observables of the N-qubit Pauli group that forms a number of commuting sets of a special kind. The proof is conveniently displayed in the form of a diagram in which the observables are represented as points (or actually as letters within circles centered at points) and the special commuting sets as lines (which could be straight or curved) joining the points. An observable is represented by a sequence of letters, each of which can be one of X, Y, Z, or I (these being the Pauli and identity operators of a qubit). For example, $XYIZZ$ represents a 5-qubit observable that is the tensor product of the observables X, Y, I, Z, and Z of the individual qubits. Every special commuting set in any of our proofs has the property that the product of all the observables in it is either $+\mathbf{I}$ or $-\mathbf{I}$, where $\mathbf{I}$ is the identity operator in the space of all the qubits. Sets with product $+\mathbf{I}$ are shown by thin lines and sets with product $-\mathbf{I}$ by thick lines in our diagrams. Any diagram representing an observables-based KS proof has the following

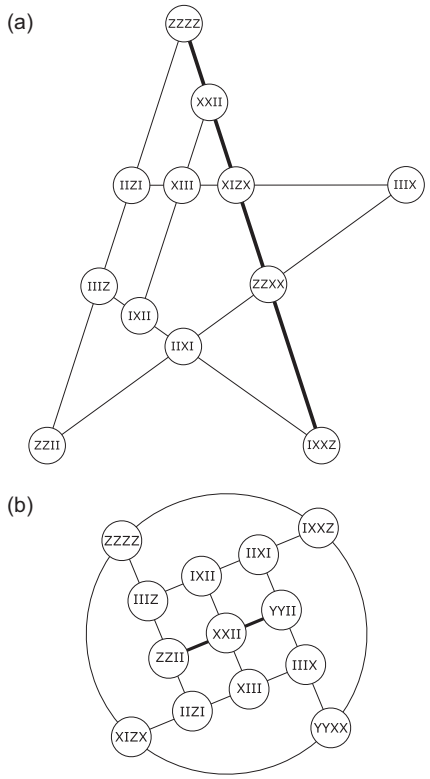

FIG. 1. Four-qubit star diagram, $\mathbf{12_2\text{-}1_5 4_4 1_3}$ (a), and 4-qubit windmill diagram, $\mathbf{13_2\text{-}5_4 2_3}$ (b).

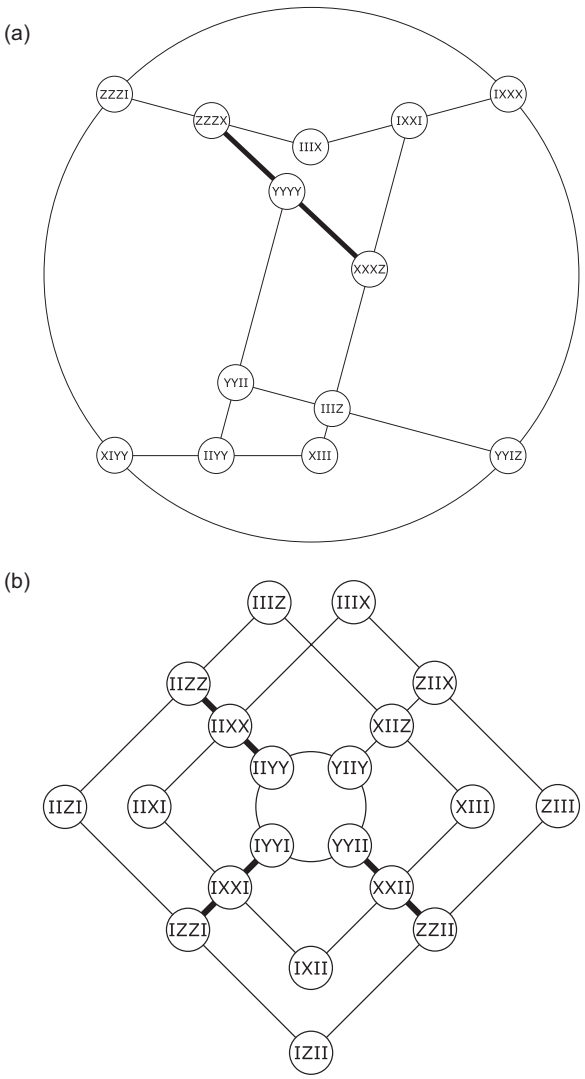

FIG. 2. Four-qubit clock diagram, $\mathbf{13_2\text{-}2_4 6_3}$ (a), and 4-qubit whorl diagram, $\mathbf{20_2\text{-}1_4 12_3}$ (b).

two properties: (A) each observable lies at the intersection of an even number of lines, and (B) the total number of thick lines is odd. These properties guarantee that the diagrams provide proofs of the KS theorem. To see why, note that the eigenvalues of any N-qubit observable are ± 1 and that a noncontextual hidden variables theory is required to assign the value $+1$ or -1 to each of the observables in such a way that the product of the values assigned to the observables on a thin (or a thick) line equals $+1$ (or -1). However properties (A) and (B) rule out such a value assignment[1] and so prove the KS theorem.

A number of N-qubit proof-diagrams are shown in Figs. 1–4 for $N = 4$, 5, and 6. The names we have given to the diagrams are whimsical and merely try to capture their shapes. We have also attached a symbol to each diagram

[1]This can be seen as follows. Let v_α be the product of the values assigned to the observables in the commuting set indexed by α and consider the product $P = \prod v_\alpha$ taken over all the commuting sets. Property (B) requires that $P = -1$ but property (A) requires that $P = +1$, so there is a contradiction.

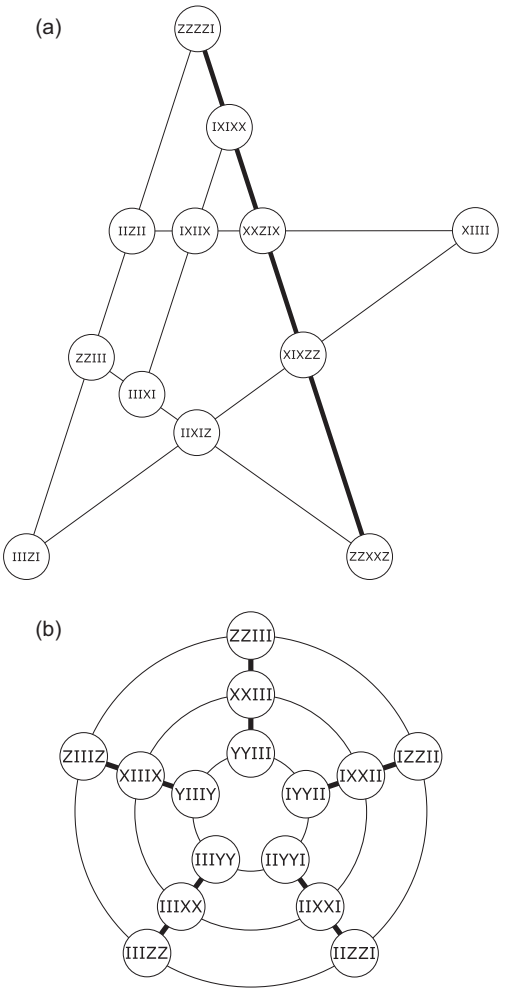

FIG. 3. Five-qubit star diagram, $\mathbf{12_2\text{-}1_5 4_4 1_3}$ (a), and 5-qubit wheel diagram, $\mathbf{15_2\text{-}3_5 5_3}$ (b).

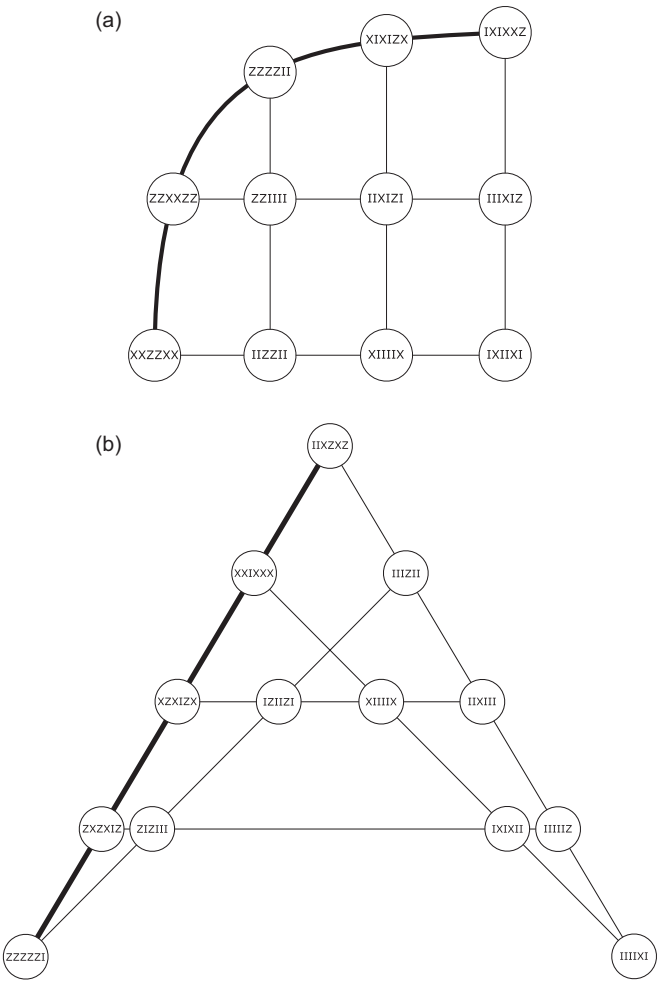

FIG. 4. Six-qubit arch diagram, $\mathbf{11_2\text{-}1_5 2_4 3_3}$ (a), and 6-qubit arrow diagram, $\mathbf{13_2\text{-}2_5 4_4}$ (b).

that should help the reader pick out the commuting sets in it (particularly in the case of the more complicated diagrams). The left half of each symbol lists the number of observables of each multiplicity (with the multiplicities as subscripts) and the right half lists the number of commuting sets of each size (with the sizes as subscripts). For example, the symbol $\mathbf{12_2\text{-}1_5 4_4 1_3}$ for the 4-qubit star diagram of Fig. 1 indicates that it contains 12 observables of multiplicity 2 (i.e., that each occur twice among its commuting sets) and that there are four commuting sets of 4 observables and one each of 5 and 3 observables. The sum of the products of each number with its subscript in the left half of the symbol must equal the similar sum of products on the right, and this can be used as a quick check on the consistency of the symbol. For a symbol to represent a valid KS proof, all the subscripts in its left half must be even (it is also necessary that the number of commuting sets with product $-\mathbf{I}$ be odd, but this fact is not made evident in the symbol and can only be checked by looking at the diagram.)

The proof diagrams we have shown here are just a small fraction of the ones we have discovered. We hope to make a more extensive collection available at a website we plan to set up.

III. PROJECTORS-BASED KS PROOFS

Each of the observables-based proofs of the previous section can be used to generate a large number of projectors-based proofs of the KS theorem. We illustrate how this can be done by considering one particular case in detail, namely, the 4-qubit star diagram of Fig. 1. The procedure for obtaining the projectors-based proofs is as follows.

(1) First enumerate the projectors that are the simultaneous eigenstates of the various sets of commuting observables in the proof. Each commuting set defines a number of mutually orthogonal projectors that sum to the identity and that we term a "pure" basis. The 4-qubit star diagram consists of six commuting sets and so gives rise to 6 pure bases. However these bases are of different sizes, with four consisting of 8 rank-2 projectors, one of 16 rank-1 projectors, and one of 4 rank-4 projectors. We now establish a numbering scheme for the projectors. To do this we label the projectors of each commuting set by their eigenvalues with respect to the observables of that set and then convert the eigenvalue strings into binary strings by the replacement $+1 \to 0, -1 \to 1$ and finally arrange the binary strings in ascending order after ignoring the digit at the extreme right. With the projectors within each commuting set ordered in this fashion, we then

number the projectors sequentially from 1 up,beginning with the first commuting set and proceeding to the others. This procedure is illustrated in Table I for the 4-qubit star diagram, whose commuting sets are shown in the first column. As an example of the numbering procedure, the projectors corresponding to the observables in the last row are represented by the binary strings 000, 011, 101, and 110 (which are arranged in ascending order according to their first two digits) and assigned the numbers 49 to 52, respectively (since the numbers 1 to 48 have already been taken by the earlier projectors).

(2) In addition to the pure bases, the projectors form a number of "hybrid" bases that consist of mixtures of projectors from different pure bases (the hybrid bases, like the pure bases, consist of sets of mutually orthogonal projectors that sum to the identity). In order to construct the hybrids, it is necessary to be able to pick out orthogonalities between projectors belonging to different pure bases. This can be done by using the following rule: two projectors from different pure bases are orthogonal if and only if they are eigenstates of one or more common observables with differing eigenvalues for at least one of those observables. As an example, projector 3 of the first row of Table I (which is represented by the binary string 00101) is orthogonal to projector 21 of the second row (which is represented by the string 1001) because they have opposite eigenvalues for the observable $ZZZZ$. Using this rule it is easy to pick out all the hybrid bases formed by the projectors in Table I and these are listed, along with the 6 pure bases, in Table II. Note that each hybrid basis is made up of the halves of two pure bases, whose other halves make up a second hybrid complementary to the first one. Complementary hybrids are listed next to each other in Table II and bear the same number, but are distinguished by the letters a and b.

TABLE I. The projectors of the 4-qubit star diagram. The projectors are the simultaneous eigenstates of the mutually commuting observables in each of the rows and are numbered as explained in the text. The product of the eigenvalue signatures of the projectors in the first row is -1, while it is $+1$ for the projectors in each of the last five rows. The ranks of the projectors associated with each commuting set are shown in the last column.

Observables	Projectors	Rank
$ZZZZ, ZZXX, XXII, XIZX, IXXZ$	1–16	1
$ZZZZ, ZZII, IIZI, IIIZ$	17–24	2
$ZZXX, ZZII, IIXI, IIIX$	25–32	2
$XIZX, IIZI, XIII, IIIX$	33–40	2
$IXXZ, IIIZ, IXII, IIXI$	41–48	2
$XXII, XIII, IXII$	49–52	4

TABLE II. The 30 bases formed by the 52 projectors of the 4-qubit star diagram. They consist of 6 pure bases (shown above the line) and 24 hybrid bases (shown below the line), with the bases numbered as shown at the left. The hybrid bases come in complementary pairs, with the members of a pair bearing the same number and being distinguished by the letters a and b.

Index	Projectors in basis															
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	17	18	19	20	21	22	23	24								
3	25	26	27	28	29	30	31	32								
4	33	34	35	36	37	38	39	40								
5	41	42	43	44	45	46	47	48								
6	49	50	51	52												
7a	1	2	3	4	5	6	7	8	21	22	23	24				
7b	9	10	11	12	13	14	15	16	17	18	19	20				
8a	1	2	3	4	9	10	11	12	29	30	31	32				
8b	5	6	7	8	13	14	15	16	25	26	27	28				
9a	1	3	5	7	9	11	13	15	37	38	39	40				
9b	2	4	6	8	10	12	14	16	33	34	35	36				
10a	1	4	6	7	10	11	13	16	41	42	43	44				
10b	2	3	5	8	9	12	14	15	45	46	47	48				
11a	1	2	5	6	9	10	13	14	51	52						
11b	3	4	7	8	11	12	15	16	49	50						
12a	17	18	21	22	27	28	31	32								
12b	19	20	23	24	25	26	29	30								
13a	17	19	21	23	35	36	39	40								
13b	18	20	22	24	33	34	37	38								
14a	17	20	22	23	43	44	47	48								
14b	18	19	21	24	41	42	45	46								
15a	25	28	30	31	34	35	37	40								
15b	26	27	29	32	33	36	38	39								
16a	25	27	29	31	42	43	45	48								
16b	26	28	30	32	41	44	46	47								
17a	33	35	37	39	50	52										
17b	34	36	38	40	49	51										
18a	41	43	45	47	50	51										
18b	42	44	46	48	49	52										

TABLE III. The 10 different types of projectors-based KS proofs contained in the 4-qubit star diagram of Fig. 1. The second and third columns give the number of projectors and bases in each proof, while the fourth column gives the detailed symbol of the proof (see text for explanation). The fifth column lists the number of distinct proofs of each type, with the sum of all the numbers in this column being $4096 = 2^{12}$.

Index	Projectors	Bases	Symbol	Count
1	47	13	$5_2^1 10_4^1 1_6^1 24_2^2 4_4^2 3_2^4$-$1_{16} 4_{12} 1_{10} 5_8 2_6$	128
2	47	13	$10_2^1 5_4^1 22_2^2 7_4^2 3_2^4$-$4_{12} 1_{10} 6_8 2_6$	512
3	47	13	$10_2^1 5_4^1 24_2^2 4_4^2 3_2^4 1_4^4$-$4_{12} 1_{10} 5_8 2_6 1_4$	128
4	49	15	$5_2^1 10_4^1 1_6^1 20_2^2 10_4^2 3_2^4$-$1_{16} 4_{12} 1_{10} 7_8 2_6$	768
5	49	15	$5_2^1 10_4^1 1_6^1 22_2^2 7_4^2 3_2^4 1_4^4$-$1_{16} 4_{12} 1_{10} 6_8 2_6 1_4$	512
6	49	15	$10_2^1 5_4^1 18_2^2 13_4^2 3_2^4$-$4_{12} 1_{10} 8_8 2_6$	512
7	49	15	$10_2^1 5_4^1 20_2^2 10_4^2 3_2^4 1_4^4$-$4_{12} 1_{10} 7_8 2_6 1_4$	768
8	51	17	$5_2^1 10_4^1 1_6^1 16_2^2 16_4^2 3_2^4$-$1_{16} 4_{12} 1_{10} 9_8 2_6$	128
9	51	17	$5_2^1 10_4^1 1_6^1 18_2^2 13_4^2 3_2^4 1_4^4$-$1_{16} 4_{12} 1_{10} 8_8 2_6 1_4$	512
10	51	17	$10_2^1 5_4^1 16_2^2 16_4^2 3_2^4 1_4^4$-$4_{12} 1_{10} 9_8 2_6 1_4$	128

(3) The system of projectors and bases yielded by any observables-based KS proof contains a large number of projectors-based parity proofs. Any projectors-based parity proof consists of an odd number of bases with the property that each of the projectors that occurs in them occurs in an even number of them. This condition guarantees that it is impossible to assign noncontextual 0/1 values to the projectors in such a way that each basis has exactly 1 projector assigned the value 1 in it, which proves the KS theorem.

It is useful to have a symbol for the system of projectors and bases that results from any observables-based KS proof. We use a symbol consisting of two halves, with the left half listing the properties of the projectors and the right half the properties of the bases. Each number in the left half represents the number of projectors of a particular rank and multiplicity (with the rank indicated as a superscript and the multiplicity as a subscript), and each number in the right half represents the number of bases of a particular size (with the size indicated as a subscript). As an example, the symbol for the system in Table II is $16_6^1 32_5^2 4_4^4$-$1_{16} 8_{12} 2_{10} 14_8 4_6 1_4$ and it indicates, among other things, that there are 32 rank-2 projectors of multiplicity 5 and 14 bases of 8 projectors in this system. We use a similar symbol to denote any projectors-based parity proof.[2]

We are now in a position to explain how all the projectors-based proofs listed in Table III can be picked out from the bases in Table II. All one has to do is to pick one member from each pair of complementary hybrids (which can be done in 2^{12} ways) and supplement them with the needed pure bases to complete the proof. As an example, suppose one picks the 12 hybrids shown in the first row of Table IV. One finds that all the projectors that occur in these bases occur an even number of times among them, with the exception of projectors 1 through 16, which each occur either once or thrice; it is then clear that one should pick pure basis 1 to ensure that all the projectors occur an even number of times among the bases (and also that the total number of bases is odd). This yields the proof shown in the first row of Table IV, whose symbol is indicated in the first row of Table III. There are 128 different proofs of this kind, as noted in the last column of Table III. By picking all possible combinations of hybrid bases, it is possible to generate all the proofs listed in Table III. It is interesting to note that while there are several proofs involving the same total number of projectors and bases, their detailed structure (as revealed by their symbols) is quite different.

This completes our description of the procedure for generating projectors-based proofs from observables-based ones. The generation of the basis table associated with an observables-based proof (the equivalent of Table II) takes a bit of effort, but once it is in hand the rest of the process is quite painless. A particularly simple type of observables-based proof is one in which each observable occurs in exactly two commuting sets and any two commuting sets have at most one observable in common (the proofs in Figs. 1–4 are all of this type). If O is the number of observables in such a proof, it is not difficult to show that the number of hybrid basis pairs is also O and the number of projectors-based proofs associated with this system is 2^O. Table V illustrates this remark by listing the number of projectors-based proofs associated with each of the observables-based proofs of Figs. 1–4. The reader should

[2]Note that we use bold font for the symbols of the observables-based proofs listed and ordinary font for the symbols of the projectors-based proofs in order to avoid any confusion between them.

TABLE IV. One example of each of the 10 different types of projectors-based proofs listed in Table III. The bases in each proof are labeled using the notation of Table II.

Index	Bases in example proof																
1	7a	8a	9a	10a	11a	12a	13a	14b	15a	16a	17b	18b	1				
2	7a	8a	9a	10a	11b	12a	13a	14a	15a	16a	17b	18a	2				
3	7a	8a	9a	10a	11b	12a	13a	14b	15a	16a	17b	18b	6				
4	7a	8a	9a	10a	11a	12a	13a	14a	15a	16a	17a	18a	1	2	4		
5	7a	8a	9a	10a	11a	12a	13a	14a	15a	16a	17b	18a	1	2	6		
6	7a	8a	9a	10a	11b	12a	13a	14a	15a	16a	17a	18b	2	4	5		
7	7a	8a	9a	10a	11b	12a	13a	14a	15a	16a	17a	18a	2	4	6		
8	7a	8a	9a	10a	11a	12a	13a	14a	15a	16b	17a	18a	1	2	3	4	5
9	7a	8a	9a	10a	11a	12a	13a	14a	15a	16a	17a	18b	1	2	4	5	6
10	7a	8a	9a	10a	11b	12a	13a	14a	15a	16b	17a	18a	2	3	4	5	6

TABLE V. For each of the observables-based proofs of Figs. 1–4, the fourth column shows the number of pure and hybrid bases formed by the projectors and the fifth column shows the total number of projectors-based parity proofs in that system.

Proof	Diagram	Symbol	Pure/hybrid bases	Parity proofs
4-qubit star diagram	Fig. 1	$\mathbf{12_2\text{-}1_5 4_4 1_3}$	6/24	$2^{12} = 4096$
4-qubit windmill diagram	Fig. 1	$\mathbf{13_2\text{-}5_4 2_3}$	7/26	$2^{13} = 8192$
4-qubit clock diagram	Fig. 2	$\mathbf{13_2\text{-}2_4 6_3}$	8/26	$2^{13} = 8192$
4-qubit whorl diagram	Fig. 2	$\mathbf{20_2\text{-}1_4 12_3}$	13/40	$2^{20} = 1048576$
5-qubit star diagram	Fig. 3	$\mathbf{12_2\text{-}1_5 4_4 1_3}$	6/24	$2^{12} = 4096$
5-qubit wheel diagram	Fig. 3	$\mathbf{15_2\text{-}3_5 5_3}$	8/30	$2^{15} = 32768$
6-qubit arch diagram	Fig. 4	$\mathbf{11_2\text{-}1_5 2_4 3_3}$	6/22	$2^{11} = 2048$
6-qubit arrow diagram	Fig. 4	$\mathbf{13_2\text{-}2_5 4_4}$	6/26	$2^{13} = 8192$

be able to generate all the projectors-based proofs in these systems using the methods described in this section.

IV. KS PROOFS BASED ON KITE DIAGRAMS

Figure 5 shows an observables-based KS proof based on a general diagram of the kite class. There are 9 observables in the body of such a diagram and one of them also serves as the starting point of its tail, which can be of arbitrary length. It is easy to see that the diagrams of this class provide a KS proof because each observable occurs in two commuting sets and just one of the commuting sets has a product of $-\mathbf{I}$. By making suitable choices for the observables A, B, . . . , H, $I_1, \ldots, I_n$, it is possible to construct KS proofs for any number of qubits from 2 up. Before presenting specific examples of such proofs, we draw attention to a simple class of projectors-based proofs implied by Fig. 5 no matter what choices are made for the observables in it.

To do this, we first enumerate the projectors defined by the sets of commuting observables in Fig. 5 and then set up the basis table formed by them. These tasks are accomplished in the same manner as in Sec. II. Once the basis table is available, we point out a set of projectors-based proofs contained in it.

Table VI shows the sets of commuting observables in the general kite diagram of Fig. 5 and the projectors defined by them. The first four commuting sets define 4 projectors each, which are numbered from 1 to 16 and have their eigenvalue signatures indicated at the tops of the columns. The last two

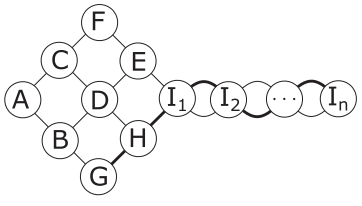

FIG. 5. The general diagram of the kite class. The four sets of three commuting observables, (A, C, F), (B, D, E), (A, B, G), and (C, D, H), have product $+\mathbf{I}$ and are shown by thin lines. The other two commuting sets have $n + 2$ observables each; the set (F, E, $I_1, \ldots, I_n$) has product $+\mathbf{I}$ and is shown by a thin line while the set (G, H, $I_1, \ldots, I_n$) has product $-\mathbf{I}$ and is shown by a thick line. Suitable choices of the observables A, B, . . . , I_n give rise to all the proofs of the kite family.

sets define projectors labeled by $n + 2$ eigenvalue signatures each, but rather than number the projectors individually we adopt the shortcut of using a single number to label all projectors having the same eigenvalues for the 3 observables in the body of the kite and differing only in their eigenvalues for the observables in the tail. Thus, for example, the number 17 denotes all projectors having eigenvalues $+1$, $+1$, $+1$ for F, E, I_1 but all possible combinations of eigenvalues for the observables $I_2, \ldots, I_n$ in the tail. The numbers from 18 to 32 are to be interpreted similarly.

The projectors in Table VI form 6 pure bases, represented by the rows of the table. Using the orthogonality rule for projectors from different pure bases (mentioned in Sec. II), it can be verified that they form the 9 pairs of complementary hybrids shown in Table VII. Table VIII shows 16 projectors-based proofs extracted from the bases of Table VII (they can be obtained by picking one member from each of the first four hybrid pairs, which can be done in 2^4 ways, and supplementing them with the required members of the remaining five hybrids). It is remarkable that any diagram of the kite class, irrespective of the length of its tail or the number of qubits it involves, always admits this set of 16 projectors-based proofs involving 9 bases each.[3] We believe that 9 is the minimum number of bases for a projectors-based proof in any dimension, but we do not have proof of this fact.

We finally give examples of N-qubit observables that can play the role of the labels A, B, C, . . . , I_n in Fig. 5. It turns out to be sufficient to specify the members of the commuting set G, H, $I_1, \ldots, I_n$, since they determine all the other observables in the manner we explain. Table IX lists the members of this set for 3 and 5 qubits before indicating its pattern for an arbitrary odd number of qubits, and Table X does the same for 4 qubits, 6 qubits, and an arbitrary even number of qubits. In each case the commuting observables are displayed horizontally, with their corresponding qubits vertically aligned. The observables G and H are always the ones whose first qubits are in bold, while the others are $I_1, \ldots, I_n$ (it is immaterial how the associations are made within these two groups). Once these observables

[3]Any kite-shaped class diagram actually gives rise to many more projectors-based proofs than just the 16 exhibited here. However the total number of proofs is not given by the 2^O rule because two of the commuting sets (namely, the ones that overlap along the tail) have more than one observable in common.

TABLE VI. Projectors defined by the kite class of diagrams of Fig. 5. The four commuting sets of observables in the upper table define the projectors 1 through 16, while the two sets in the lower table define the groups of projectors numbered 17 through 32. The eigenvalue signatures of the projectors for the defining observables are shown at the tops of the columns. The numbers 1 through 16 represent single projectors but the numbers 17 through 32 each represent an ensemble of mutually orthogonal projectors, as explained in the text. The product of the eigenvalue signatures of each of the projectors 1 through 16 is +, and the same is true of each of the members of the ensembles 17 through 24. However the product of the signatures is − for each of the members of the ensembles 25 through 32.

Observables	+ + +	+ − −	− + −	− − +
A, C, F	1	2	3	4
B, D, E	5	6	7	8
A, B, G	9	10	11	12
C, D, H	13	14	15	16

Observables	+ + + ⋯	+ + − ⋯	+ − + ⋯	+ − − ⋯	− + + ⋯	− + − ⋯	− − + ⋯	− − − ⋯
F, E, $I_1, \ldots$	17	18	19	20	21	22	23	24
G, H, $I_1, \ldots$	25	26	27	28	29	30	31	32

have been placed at their locations in the general kite diagram of Fig. 5, F and E are chosen as the observables obtained from G and H by swapping their first qubits (which are always X and Z). The observables A, B, C, and D are then uniquely determined by the requirement that they have the necessary commutation and product properties. Figure 6 (left) shows the kite diagram that results on applying this procedure to the 3-qubit observables of Table IX. The 4-qubit observables of Table X yield a kite diagram with a tail of length two, but rather than exhibiting this proof we show, in Fig. 6 (right), a more economical proof with a tail of length one.

The economy we pointed out for the 4-qubit proof extends to higher qubit proofs as well: we have found N-qubit proofs, for all $N \geqslant 3$, whose longest commuting sets involve considerably less than the $N + 1$ observables involved in the proofs of Tables IX and X. Some examples of such proofs are shown in Table XI. The 16-qubit proof has a commuting set of just 7 observables, which is much less than the 17 involved in the proof of Table X. This sort of compression allows for the design of much more economical KS tests as one goes to a large number of qubits.

V. DISCUSSION

This paper has established the following results:

(1) The hierarchy of N-qubit Pauli groups (for $N \geqslant 2$) contains many subsets of observables that provide parity proofs of the KS theorem. We restrict our attention to proofs that are irreducible (i.e., that cannot be reduced to simpler proofs by omitting some subset of observables and/or qubits in them) and unitarily inequivalent. With these caveats, the 2-qubit group gives rise to only two distinct types of proofs (the Peres-Mermin square and a more complicated structure we call the whorl, which are shown as Figs. 1 and 2 of Ref. [4]), but the 3-qubit group leads to many more [4] and the possibilities increase rapidly as one goes upwards in the number of qubits. It would be an interesting problem to make a more systematic inventory of the proofs at a given value of N and to get a feeling for how this number grows with N. There are two devices we have introduced in this paper that could assist with this task: the first is a diagrammatic representation of each proof (from which it can be verified by inspection), and the second is a symbol that captures the important features of the observables and special commuting sets in the proof. However we should caution that neither of these devices suffices to pin down a proof uniquely since there are distinct proofs that can be accommodated on the same diagrammatic skeleton, as well as inequivalent proofs that share the same symbol (see Fig. 7 of Ref. [4] for an example). Even in the absence of a detailed knowledge of the terrain, one can state quite confidently that the Pauli group (particularly as one goes to a larger number of qubits) abounds in a great variety of structures that can be used to give transparent demonstrations of quantum contextuality.

TABLE VII. Nine of the hybrid basis pairs formed by the projectors of Table VI. Complementary hybrids are shown on the same line and distinguished by the letters a and b.

Index	Projectors in basis	Index	Projectors in basis
1a	1 2 11 12	1b	3 4 9 10
2a	1 3 15 16	2b	2 4 13 14
3a	5 6 10 12	3b	7 8 9 11
4a	5 7 14 16	4b	6 8 13 15
5a	1 4 21 22 23 24	5b	2 3 17 18 19 20
6a	5 8 19 20 23 24	6b	6 7 17 18 21 22
7a	9 12 29 30 31 32	7b	10 11 25 26 27 28
8a	13 16 27 28 31 32	8b	14 15 25 26 29 30
9a	17 18 23 24 25 26 31 32	9b	19 20 21 22 27 28 29 30

TABLE VIII. The 16 projectors-based KS proofs formed by the bases of Table VII (with the bases labeled as in that table).

Index	Bases in proof								
1	1a	2a	3a	4a	5b	6b	7b	8b	9b
2	1a	2a	3a	4b	5b	6a	7b	8a	9a
3	1a	2a	3b	4a	5b	6a	7a	8b	9a
4	1a	2a	3b	4b	5b	6b	7a	8a	9b
5	1a	2b	3a	4a	5a	6b	7b	8a	9a
6	1a	2b	3a	4b	5a	6a	7b	8b	9b
7	1a	2b	3b	4a	5a	6a	7a	8a	9b
8	1a	2b	3b	4b	5a	6b	7a	8b	9a
9	1b	2a	3a	4a	5a	6b	7a	8b	9a
10	1b	2a	3a	4b	5a	6a	7a	8a	9b
11	1b	2a	3b	4a	5a	6a	7b	8b	9b
12	1b	2a	3b	4b	5a	6b	7b	8a	9a
13	1b	2b	3a	4a	5b	6b	7a	8a	9b
14	1b	2b	3a	4b	5b	6a	7a	8b	9a
15	1b	2b	3b	4a	5b	6a	7b	8a	9a
16	1b	2b	3b	4b	5b	6b	7b	8b	9b

(2) The second major point of this paper is that every observables-based KS proof can be used to generate a system of projectors and bases from which a a large number of projectors-based KS proofs can be obtained. The algorithm for generating these proofs is simple, and the proofs themselves are easy to validate because only a simple parity check is called for. We have introduced a detailed symbol for a projectors-based proof that describes the projectors and bases in it, both as a way of summarizing the key aspects of the proof and to draw attention to the wide variety of proofs that can coexist within the same framework of pure and hybrid bases provided by an observables-based proof. Since the observables-based proofs are themselves very numerous, and each spawns a large number of projectors-based proofs (typically thousands), the quantity and variety of the latter proofs vastly outstrip those of the former. We should add that the symbols we have introduced for the projectors-based proofs, though useful and informative, do not serve to pin them down uniquely since we have found many examples of inequivalent proofs that are described by the same symbol. Among all the observables-based and related projectors-based proofs, there is a simple class that is worth singling out for special mention: it is the one in which each observable occurs in exactly two commuting sets and any two commuting sets have at most one observable in common. One knows in this case, even before one has set up the basis table, that one will find exactly 2^O projectors-based proofs.

TABLE IX. Observables for a kite class proof based on 3 qubits (left), 5 qubits (middle), and an arbitrary odd number of qubits (right).

			Z	*I*	*I*	*I*	*Z*	**Z**	*I*	⋯	*I*	*Z*
Z	*I*	*Z*	*I*	*Z*	*I*	*I*	*Z*	*I*	*Z*	⋱	⋮	⋮
I	*Z*	*Z*	*I*	*I*	*Z*	*I*	*Z*	⋮	⋱	⋱	*I*	*Z*
X	*X*	*X*	*I*	*I*	*I*	*Z*	*Z*	*I*	⋯	*I*	*Z*	*Z*
Y	*Y*	*X*	**X**	*X*	*X*	*X*	*X*	**X**	⋯	*X*	*X*	*X*
			Y	*Y*	*Y*	*Y*	*X*	*Y*	⋯	*Y*	*Y*	*X*

TABLE X. Observables for a kite class proof based on 4 qubits (top left), 6 qubits (top right), and an arbitrary even number of qubits (bottom).

					Z	*Z*	*Z*	*Z*	*Z*	*Z*
Z	*Z*	*Z*	*Z*		*Y*	*Y*	*Z*	*Z*	*Z*	*Z*
Y	*Y*	*Z*	*Z*		**X**	*I*	*X*	*I*	*I*	*I*
X	*I*	*X*	*I*		*I*	*X*	*I*	*X*	*I*	*I*
I	*X*	*I*	*X*		*I*	*I*	*X*	*I*	*X*	*I*
I	*I*	*X*	*X*		*I*	*I*	*I*	*X*	*I*	*X*
					I	*I*	*I*	*I*	*X*	*X*

		Z	*Z*	*Z*	*Z*	⋯	*Z*				
		Y	*Y*	*Z*	*Z*	⋯	*Z*				
		X	*I*	*X*	*I*	⋯	*I*				
		I	*X*	*I*	*X*	⋱	⋮				
		⋮	⋱	⋱	⋱	⋱	*I*				
		I	⋯	*I*	*X*	*I*	*X*				
		I	⋯	*I*	*I*	*X*	*X*				

(3) We have discovered several infinite families of observables-based proofs (that we term the star class, the wheel class, the whorl class, and the kite class) whose members yield KS proofs for all numbers of qubits from 2 up. The kite class is the most complex of these families, and we have given a detailed discussion of it in this paper. This family has two remarkable features. The first is that for a system of N qubits it is always possible to find commuting sets of considerably less than N observables that can be used to construct a KS proof, thus leading to greater economy in the design of experimental tests based on this class of proofs. And the second is that *any* kite-shaped proof always yields a projectors-based proof involving only 9 bases (or experimental contexts). These proofs are generalizations of the classic 18-9 proof of Cabello *et al.* [9] in four dimensions and hold in all dimensions of the form 2^N, for $N \geqslant 2$. It is an open question whether there are any proofs involving less than 9 bases in these dimensions (we believe the answer is no). An even more basic question is whether there are any projectors-based parity proofs[4] at all in any even dimension not of the form 2^N. Again we suspect that the answer is no, but we do not have a proof of

[4]Nonparity proofs based on rays are known in all dimensions $\geqslant 3$ [14,15].

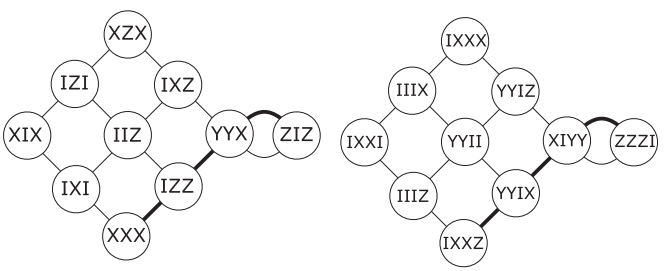

FIG. 6. Three-qubit kite diagram (left) based on the observables of Table IX and a four-qubit kite diagram (right) based on the same skeleton as at the left.

TABLE XI. Kite proofs for 7 qubits based on 5 commuting observables (top), for 11 qubits based on 6 commuting observables (middle), and for 16 qubits based on 7 commuting observables (bottom). The full proofs can be constructed by placing these observables on the skeleton of the kite in the manner explained in the text.

				Z	*Z*	*Z*	*Z*	*Z*	*I*	*I*						
				X	*X*	*Z*	*X*	*X*	*Z*	*Z*						
				Y	*I*	*X*	*Z*	*Z*	*X*	*X*						
				I	*Y*	*I*	*X*	*I*	*Z*	*X*						
				I	*I*	*X*	*I*	*X*	*X*	*Z*						
		I	*I*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*				
		Z	*I*	*Z*	*Z*	*Z*	*X*	*X*	*I*	*X*	*X*	*I*				
		I	*Z*	*X*	*X*	*I*	*Z*	*Z*	*Z*	*I*	*I*	*I*				
		X	*I*	*X*	*I*	*X*	*X*	*I*	*X*	*Z*	*X*	*X*				
		I	*X*	*I*	*X*	*I*	*I*	*X*	*I*	*I*	*Z*	*Z*				
		Y	*Y*	*I*	*I*	*X*	*I*	*I*	*X*	*X*	*I*	*X*				
Z	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*Z*	*I*	*I*	*I*	*I*	*I*	*I*	*I*	*I*	
X	*X*	*X*	*X*	*I*	*I*	*I*	*I*	*Z*	*Z*	*Z*	*Z*	*I*	*I*	*I*	*I*	
Y	*I*	*I*	*I*	*X*	*X*	*X*	*I*	*X*	*I*	*I*	*I*	*Z*	*Z*	*I*	*I*	
I	*Y*	*I*	*I*	*Y*	*I*	*I*	*I*	*I*	*X*	*X*	*X*	*X*	*I*	*Z*	*I*	
I	*I*	*I*	*I*	*I*	*Y*	*I*	*X*	*Y*	*Y*	*I*	*I*	*I*	*I*	*X*	*Z*	
I	*I*	*Y*	*I*	*I*	*I*	*I*	*Y*	*I*	*I*	*Y*	*I*	*Y*	*X*	*I*	*X*	
I	*I*	*I*	*Y*	*I*	*I*	*Y*	*I*	*I*	*I*	*I*	*Y*	*I*	*Y*	*Y*	*Y*	

this conjecture (and would find it fascinating if someone came up with a counterexample).

There is currently a great interest in contextuality and nonlocality and their experimental tests. In one interesting development, it has been shown that any projectors-based KS proof can be converted into an inequality for testing quantum contextuality [16] and a number of experimental tests of such inequalities have actually been carried out [17]. A number of works have shed light on contextuality in a manner that bypasses the KS theorem [18]. On the formal side, a connection between KS proofs and "logical Bell inequalities" has been made in Ref. [19] and the question of state-independent contextuality for identical particles has been explored in Ref. [20]. Although the present work concentrates entirely on qubits, it should be pointed out that KS proofs for qudits (i.e., d-state systems) have been explored in Ref. [21]. Among the practical applications of contextuality that are receiving attention are quantum key distribution [22], quantum error correction [23,24], random number generation [25], parity oblivious transfer [26], and the design of relational databases [27]. This is not a complete survey, of course, but should convey a feeling for the broader context in which the results reported here may be of interest.

[1] M. Waegell and P. K. Aravind, Phys. Lett. A **377**, 546 (2013).

[2] E. P. Specker, Dialectica **14**, 239 (1960); S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967); see also J. S. Bell, Rev. Mod. Phys. **38**, 447 (1966); reprinted in *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, UK, 1987).

[3] M. Waegell and P. K. Aravind, J. Phys. A: Math. Theor. **44**, 505303 (2011).

[4] M. Waegell and P. K. Aravind, J. Phys. A: Math. Theor. **45**, 405301 (2012).

[5] A. Peres, J. Phys. A **24**, L175 (1991).

[6] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990); Rev. Mod. Phys. **65**, 803 (1993).

[7] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989); D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[8] M. Waegell and P. K. Aravind, Found. Phys. **41**, 1786 (2011).

[9] A. Cabello, J. M. Estebaranz, and G. García-Alcaine, Phys. Lett. A **212**, 183 (1996).

[10] M. Kernaghan, J. Phys. A **27**, L829 (1994).

[11] M. Pavičić, N. D. Megill, and J. P. Merlet, Phys. Lett. A **374**, 2122 (2010); M. Pavičić, J. P. Merlet, B. D. McKay, and N. D. Megill, J. Phys. A **38**, 1577 (2005); M. Pavičić, J. P. Merlet, and N. D. Megill, The French National Institute for Research in Computer Science and Control Research Reports RR-5388 (2004).

[12] M. Waegell and P. K. Aravind, J. Phys. A: Math. Theor. **44**, 505303 (2011); M. Waegell, P. K. Aravind, N. D. Megill, and M. Pavičić, Found. Phys. **41**, 883 (2011).

[13] M. Kernaghan and A. Peres, Phys. Lett. A **198**, 1 (1995).

[14] A. Cabello, J. M. Estebaranz, and G. Garcia-Alcaine, Phys. Lett. A **339**, 425 (2005).

[15] J. Zimba and R. Penrose, Stud. Hist. Philos. Sci. **24**, 697 (1993).

[16] A. Cabello, Phys. Rev. Lett. **101**, 210401 (2008); P. Badziąg, I. Bengtsson, A. Cabello, and I. Pitowsky, *ibid.* **103**, 050401 (2009).

[17] G. Kirchmair, F. Zähringer, R. Gerritsma, M. Kleinmann, O. Gühne, A. Cabello, R. Blatt, and C. F. Roos, Nature (London) **460**, 494 (2009); H. Bartosik, J. Klepp, C. Schmitzer, S. Sponar, A. Cabello, H. Rauch, and Y. Hasegawa, Phys. Rev. Lett. **103**, 040403 (2009); E. Amselem, M. Rådmark, M. Bourennane, and A. Cabello, *ibid.* **103**, 160405 (2009); O. Moussa, C. A. Ryan, D. G. Cory, and R. Laflamme, *ibid.* **104**, 160501 (2010).

[18] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky, Phys. Rev. Lett. **101**, 020403 (2008); Y. C. Liang, R. W. Spekkens, and H. M. Wiseman, Phys. Rep. **506**, 1 (2011); P. Badziąg, I. Bengtsson, A. Cabello, H. H. Granström, and J.-Å. Larsson, Found. Phys. **41**, 414 (2011); S. Yu and C. H. Oh, Phys. Rev. Lett. **108**, 030402 (2012); arXiv:1112.5513.

[19] S. Abramsky and L. Hardy, Phys. Rev. A **85**, 062114 (2012).

[20] A. Cabello and M. T. Cunha, Phys. Rev. A **87**, 022126 (2013).

[21] N. J. Cerf, S. Massar, and S. Pironio, Phys. Rev. Lett. **89**, 080402 (2002).

[22] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000); K. Svozil, arXiv:0903.0231; A. Cabello, V. DAmbrosio, E. Nagali, and F. Sciarrino, Phys. Rev. A **84**, 030302(R) (2011).

[23] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, and C. H. Oh, Phys. Rev. A **78**, 012306 (2008).

[24] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[25] K. Svozil, Phys. Rev. A **79**, 054306 (2009).

[26] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Phys. Rev. Lett. **102**, 010401 (2009).

[27] S. Abramsky, arXiv:1208.6416.