12-19-2022

Golay Codes and Quantum Contextuality

Mordecai Waegell
Chapman University, waegell@chapman.edu

P. K. Aravind
Worcester Polytechnic Institute

Recommended Citation

M. Waegell and P. K. Aravind, Golay codes and quantum contextuality, Phys. Rev. A **106**, 062421 (2022). https://doi.org/10.1103/PhysRevA.106.062421

Golay Codes and Quantum Contextuality

Golay codes and quantum contextuality

Mordecai Waegell[1,*] and P. K. Aravind[2,†]
[1]*Institute for Quantum Studies, Chapman University, Orange, California 92866, USA*
[2]*Physics Department, Worcester Polytechnic Institute, Worcester, Massachusetts 01609, USA*

(Received 10 June 2022; accepted 12 October 2022; published 19 December 2022)

It is shown that the codewords of the binary and ternary Golay codes can be converted into rays in $\mathbb{RP}^{23}$ and $\mathbb{RP}^{11}$ that provide proofs of the Kochen-Specker theorem in real state spaces of dimensions 24 and 12, respectively. Some implications of these results are discussed.

DOI: 10.1103/PhysRevA.106.062421

I. INTRODUCTION

In 1949, Golay [1–4] discovered two remarkable error-correcting codes, a binary code, now designated by the symbol[1] **[24,12,8]**, consisting of $2^{12} = 4096$ codewords of 24 characters (each a 0 or 1) with a minimum distance[2] of 8 between the codewords, and a ternary code, with symbol **[12,6,6]**, consisting of $3^6 = 729$ codewords of 12 characters (each a 0, 1, or 2) with a minimum distance of 6 between the codewords.[3] These codes led to significant advances in coding theory and mathematics in the decades following their discovery. In coding theory the Golay codes have the distinction of being the only perfect codes over finite fields that can correct more than a single error in their codewords.[4] In mathematics, the binary Golay code led to the discovery of the remarkable Leech lattice [5] in 24 dimensions that provides the densest packing of identical spheres in this dimension [6] (the only other dimension in which such a packing is known being 8). In addition, in group theory, as Preskill [4] put it, the Golay codes set in motion the entire sequence of events that led to the complete classification of the finite groups (including particularly the "sporadic" groups) in the last part of the previous century.

The advent of quantum computing and the resulting interest in quantum error correction led to a renewed interest in classical cryptography when it was realized that many of the results of the latter could be adapted and put to use in the quantum context. When the first quantum error-correcting codes were proposed, it was natural to wonder if, in addition to their practical utility, they could be used to shed light on any of the fundamental mysteries of quantum mechanics. This question seems to have been first considered by DiVincenzo and Peres [8], who answered it in the affirmative.[5] They showed that the five-qubit codewords representing logical bits in the quantum code proposed in [9,10] could be used to give proofs of the Bell nonlocality [11] and Kochen-Specker-Bell [12] theorems, in the spirit of the proofs that were given earlier by Greenberger, Horne, and Zeilinger [13] and Mermin [14]. They pointed out that the seven-qubit codewords of Steane [15] also gave rise to such proofs and surmised that other quantum codewords would as well since they invariably involved entangled states of three or more qubits. Because of the last observation, the connection between quantum error-correcting codes and quantum paradoxes (i.e., the Bell and Kochen-Specker theorems), though of great interest, is perhaps not entirely unexpected.

However, is there any connection between classical error-correcting codes and the quantum paradoxes mentioned above? No obvious example comes to mind. It is the purpose of this paper to show that the codewords of the two Golay codes can be converted into rays in state spaces of dimension 24 and 12 that provide proofs of the Kochen-Specker (KS) theorem in these dimensions. The proofs are simple and follow from the impossibility of solving certain Diophantine equations.

Since numerous proofs of the KS theorem in all dimensions from three up are known [16], the discovery of yet another example might not occasion much surprise. Nevertheless, the present demonstration may be of interest because it reveals a surprising connection between classical error-correcting codes and quantum contextuality, two subjects that are not usually thought of as being related to each other. A further

*waegell@chapman.edu
†paravind@wpi.edu

[1]The symbol we use for classical error-correcting codes is standard and consists of three numbers placed within square brackets. We will use bold font for this symbol whenever it occurs so that it is not confused with the references.

[2]The (Hamming) distance between two codewords is the number of places in which they differ.

[3]These codes are actually "extended" codes obtained from the codes **[23,12,7]** and **[11,6,5]** of length 23 and 11, respectively, by the addition of a parity check digit. The latter codes are sometimes referred to as "punctured" codes.

[4]The maximum number of errors that can be corrected in the binary or ternary codes is three or two, respectively.

[5]It is interesting to note that Shor [7] went in the reverse direction by using the three-qubit GHZ-Mermin codewords, which were used to prove the Bell and Kochen-Specker theorems, to propose one of the earliest quantum error-correcting codes.

TABLE I. Generator matrix for the binary Golay code (taken from Ref. [2]), with the 12×12 identity matrix split off at the left. The rows are numbered 1 to 12 from top to bottom and the codewords can be constructed from them via Eq. (1).

1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1	1	0	1	1
0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	1	1	1	0	1
0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	1	1	1	1
0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	1	1	1
0	0	0	0	1	0	0	0	0	0	0	0	1	1	0	1	1	0	1	0	0	0	1	1
0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	0	1	1	0	1	0	0	0	1
0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	0	1	1	0	1	0	0	1
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	0	1	1	0	1	0	1
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	0	1	1	0	1	1
0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	1	1	0	1	1	0	1
0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	1	1	0	1	1	1
0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0

discussion of this point will be given after our main results are first presented.

II. BINARY GOLAY CODE AND THE KS THEOREM IN 24 DIMENSIONS

Table I shows a generator matrix for the binary Golay code. The $2^{12} = 4096$ codewords can be obtained from it as

$$w(n) = \sum_{i=1}^{12} a_{n,i} v_i, \tag{1}$$

where v_i is the ith row of the matrix, $a_{n,i} \in (0, 1)$, the sum over i is done bitwise modulo 2, and we introduced the integer

$$n = \sum_{i=1}^{12} a_{n,i} 2^{12-i} + 1 \tag{2}$$

to label the codeword $a_{n,1} a_{n,2} \ldots a_{n,12}$ (note that n is one more than the decimal integer defined by the codeword).

We next convert each codeword into a ray in $\mathbb{RP}^{23}$ by replacing each 1 in it by a -1 and each 0 by a 1. Since the codewords n and 4097–n are the complements of each other (i.e., have their 0's and 1's exchanged), they map into the same ray, which we will denote by the integer n. The codewords of the binary Golay code then give rise to a system of 2048 rays in $\mathbb{RP}^{23}$, which we will label by the integers 1 through 2048. These rays form a large number of bases (i.e., sets of 24 mutually orthogonal rays), and it is these bases that we must look at to find proofs of the KS theorem.

A proof of the KS theorem [16,18] requires finding a set of bases such that each of the rays in them cannot be assigned the value 0 or 1 in a noncontextual[6] manner in such a way that every basis has exactly one ray assigned the value 1 in it.[7] However, the number of bases formed by the 2048 rays is so large (in the tens of thousands, at the very least) that any hope of finding a subset of them that yields a proof of the KS theorem seems futile. However, we found a way around this obstacle.

First note two elementary facts: (i) two codewords at a distance of 12 from each other correspond to orthogonal rays and (ii) a set of 24 codewords, any two of which are a distance 12 apart, make up a basis.

Now each codeword has 2576 others at a distance of 12 from it, and it is not hard to pick out a basis from this set. One such basis is shown in the first row of Table II, with each ray represented by its integer label. From this "seed" basis, one can generate a system of 2048 bases by adding the ray n, for $1 \leqslant n \leqslant 2048$, to each ray of the basis (to do this, replace each ray by its codeword, add the codewords bitwise modulo 2 and replace the resulting codeword by its ray.) It is obvious that this procedure generates bases because adding the same codeword to two codewords does not change the distance between them. If one lists all the bases obtained in this way starting from the seed basis, one gets a table like that in Table II, in which only a few of the bases are shown. This table can be thought of as a 2048×24 matrix whose elements are rays and whose rows are bases. It follows from the fact that the Golay code is a linear code that each ray occurs exactly once in every column of the matrix, and therefore 24 times over the entire matrix. Thus this system of rays and bases can be described by the symbol 2048_{24}–2048_{24}, in which the numbers represent the rays and bases and the subscripts the incidence of each type of object with the other.

The proof of the KS theorem follows immediately from this symbol because the total number of bases, 2048, is not divisible by the number of bases in which each ray occurs, or 24, making it impossible to have just one ray with the value 1 in each basis.

Some comments are in order about this proof.

(1) It may not be the most economical proof in that there may be a subset of the bases that yields a briefer proof. Exploring all the subsets is an onerous task, both in view of the large number of bases and the high dimensionality of the space involved, so we proceed as follows. We pick n mutually orthogonal rays and look at all rays orthogonal to them to obtain a subset of the 2048 rays that live in a $(24 - n)$-dimensional space, and then try to find a KS proof in the resulting system of rays and bases. For $n \geqslant 4$ the number of rays and bases shrink to the point where this possibility is easily ruled out, but for $n \leqslant 3$ (i.e., in dimensions 21 through 23) the number of bases is large enough that the matter cannot be settled without a more detailed investigation.

(2) The proof we give above is based on the bases of Table II. However, the rays of the Golay code give rise to many other bases, and it is possible that the complete set of bases may house both a larger number and greater variety of KS proofs than the particular set we considered. It would be particularly interesting to find the smallest proof (in terms of the number of bases or contexts) yielded by this code.

(3) The "punctured" code **[23,12,7]**, obtained from the binary code by dropping the parity check digit, is of no interest in connection with the KS theorem because, if its codewords are converted into rays in $\mathbb{RP}^{22}$ in the same manner as before, no orthogonal pairs of rays result.

[6]The term "noncontextual" means that each ray assumes the same value in all the bases in which it occurs.

[7]The sets of bases yielding proofs of the KS theorem are often simply referred to as KS sets. We will use the terms KS proofs and KS sets interchangeably in this paper.

TABLE II. The 2048 bases obtained from a "seed" basis (the one in the first row) by adding all the rays to it in the manner described in the text.

1	127	128	136	177	414	586	788	866	911	1005	1011	1225	1323	1324	1366	1491	1510	1589	1607	1704	1722	1756	1821
2	128	127	135	178	413	585	787	865	912	1006	1012	1226	1324	1323	1365	1492	1509	1590	1608	1703	1721	1755	1822
3	125	126	134	179	416	588	786	868	909	1007	1009	1227	1321	1322	1368	1489	1512	1591	1605	1702	1724	1754	1823
										...	...	...											
2048	1922	1921	1913	1872	1635	1463	1261	1183	1138	1044	1038	824	726	725	683	558	539	460	442	345	327	293	228

III. TERNARY GOLAY CODE AND THE KS THEOREM IN 12 DIMENSIONS

Table III shows a generator matrix for the ternary Golay code. The $3^6 = 729$ codewords can be obtained from it as

$$\sum_{i=1}^{6} a_{n,i} v_i, \tag{3}$$

where v_i is the ith row of the matrix, $a_{n,i} \in (-1, 0, 1)$, and the addition is done tritwise modulo 3. The label n refers to the codeword $a_{n,1} \ldots a_{n,6}$, but we do not introduce an integer for it as we have no need for it below.

If one ignores the codeword with all 0's, the others come in pairs that are the negatives of each other, and keeping only one member of each pair gives a system of 364 rays in $\mathbb{RP}^{11}$. A computer program shows that these rays form 140 647 bases (or sets of 12 mutually orthogonal rays), with 132 rays occurring in 9496 bases, 220 rays in 27 bases, and 12 rays in 35 696 bases, so that the system can be characterized by the symbol $132_{9496}220_{27}12_{35696}$–$140\,647_{12}$ (note that the sum of the products of the numbers and their subscripts on the left equals the similar product on the right). However, this symbol gives a proof of the KS theorem for the following reason.

A noncontextual hidden variables theory requires a 1 to be assigned to a certain number of rays of each of the three types so that every basis has exactly one ray assigned the value 1 in it. But if x, y, and z are the numbers of rays of the three types assigned a 1, a successful value assignment requires that there be at least one solution to the Diophantine equation $9496x + 27y + 35696z = 140\,647$ subject to the constraints $0 \leqslant x \leqslant 132$, $0 \leqslant y \leqslant 220$ and $0 \leqslant z \leqslant 12$. However, it is easily checked that no such solution exists, and this proves the theorem.

It is actually possible to give a much quicker proof of the theorem by considering only the 220 rays arising from the 440 codewords of weight 9, which form a total of 495 bases, with each ray occurring in exactly 27 bases (see the Supplemental Material [19] for a listing of these rays and their bases). Thus this system can be described by the symbol 220_{27}–495_{12}. However, since the total number of bases, 495, is not divisible by the number of bases in which each ray occurs, or 27, the theorem is proved.

It would be interesting to find the smallest KS proof provided by the ternary Golay code. It may occur within the 495 bases formed by the codewords of weight 9 or the much larger set of bases formed by all the codewords. The "punctured" code **[11,6,5]** leads to no bases in 11 dimensions, but it does lead to a large number of bases in 10 dimensions or less and so may harbor KS sets there. We also examined an alternative mapping of the words into rays, in which the digits 0, 1, and -1 are mapped into the cube roots of unity, but found that it fails to lead to any proofs of the KS theorem [20].

TABLE III. Generator matrix for the ternary Golay code (taken from Ref. [2]), with the 6×6 identity matrix split off at the left. The rows are numbered 1 to 6 from top to bottom and the codewords can be constructed from them via Eq. (3). Note: $\bar{1} = -1$.

1	0	0	0	0	0	0	1	1	1	1	1
0	1	0	0	0	0	$\bar{1}$	0	1	$\bar{1}$	$\bar{1}$	1
0	0	1	0	0	0	$\bar{1}$	1	0	1	$\bar{1}$	$\bar{1}$
0	0	0	1	0	0	$\bar{1}$	$\bar{1}$	1	0	1	$\bar{1}$
0	0	0	0	1	0	$\bar{1}$	$\bar{1}$	$\bar{1}$	1	0	1
0	0	0	0	0	1	$\bar{1}$	1	$\bar{1}$	$\bar{1}$	1	0

IV. DISCUSSION

We showed that the codewords of the binary and ternary Golay codes can be mapped into rays in real Hilbert spaces of dimension 24 and 12 that provide proofs of the Kochen-Specker theorem in these dimensions. The proofs work by showing that the solutions to certain Diophantine equations, supplemented by a constraint in one case, do not exist. Table IV gives an overview of the three proofs presented in the paper.

Despite the fact that it is over half a century old, the Kochen-Specker theorem continues to be of great interest because of the issue of contextuality it has brought to the fore. A recent article by Budroni *et al.* [16] provides a comprehensive overview of the KS theorem and contextuality from a contemporary viewpoint, discussing both how the notion of contextuality has evolved over the years and the many uses to which it has been put. On the foundational front, early work on contextuality focused mainly on finding definitive proofs of it based on contradictions between the answers to certain sets of yes-no questions, whereas current efforts have shifted more in the direction of demonstrating it unambiguously in the face of theoretical objections [21] to the definitive proofs as well as the practical limitations of experimental tests. This shift of focus has led to the development of noncontextuality inequalities [22,23] as well as operationally motivated definitions of noncontextuality [24] that can lead to more decisive experimental tests [25]. As far as its applications are concerned, contextuality has been shown to be the source of speedup in quantum computations of various kinds [26], to guarantee the security of quantum key distribution protocols in a device-independent manner [27], and to be a resource for random number generation [28], among other things [16].

Against this backdrop, what is the interest and significance of the results presented here? They clearly belong to the category of definitive proofs mentioned above in which

TABLE IV. KS proofs based on the binary and ternary Golay codes. The first column lists the code from which the proof is derived, the second the system of rays and bases used in the proof, and the third the Diophantine equation, together with any constraints, whose insolubility constitutes the proof.

Code	Rays-Bases	Diophantine equation
Binary Golay code **[24,12,8]**	2048_{24}–2048_{24} All rays and the 2048 bases obtained by adding all the codewords to a fixed basis	$24x = 2048$
Ternary Golay code **[12,6,6]**	$132_{9496}220_{27}12_{35696}$–$140647_{12}$ All rays and their bases	$9496x + 27y + 35696z = 140\,647$ $0 \leqslant x \leqslant 132, 0 \leqslant y \leqslant 220, 0 \leqslant z \leqslant 12$
Ternary Golay code **[12,6,6]**	220_{27}–495_{12} Rays corresponding to codewords of weight 9 and their bases	$27x = 495$

interest has now waned because so many of them are known. Nevertheless, we would like to argue that our results are of interest for at least a couple of reasons. For one thing, definitive proofs still offer one route to the formulation of noncontextuality inequalities and so new proofs are worth noting in case they lead to better experimental tests or are more suited to a particular application. However, a more significant reason, in our opinion, is that they reveal a surprising connection between classical error-correcting codes and the seemingly unrelated subject of quantum contextuality. This connection, which is indicated by the dashed arrow in Fig. 1, completes the triangular linkage between the three concepts shown there.

One might wonder if there are other classical codes that allow the connection indicated by the dashed arrow to be made. A clue is provided by the following generalization of the construction we gave earlier based on the binary Golay code. Consider a binary linear code with the symbol **[2n,k,d]**. This code can be made to yield 2^{k-1} rays in $\mathbb{RP}^{2n-1}$ by the same method that was used for the Golay code. Now, if the code has $2n$ codewords that are at a distance of n from each other, then the rays corresponding to these words form a basis and successively adding each of the 2^{k-1} rays to this basis[8] yields a total of 2^{k-1} bases in which each of the rays occurs exactly $2n$ times. But if 2^{k-1} is not divisible by $2n$, no satisfactory 0/1 assignment to the rays is possible and this proves the KS theorem. To summarize, the KS theorem can be proved by finding a binary linear code, **[2n,k,d]**, for which 2^{k-1} is not divisible by $2n$ and which also has $2n$ codewords at a distance of n from each other.

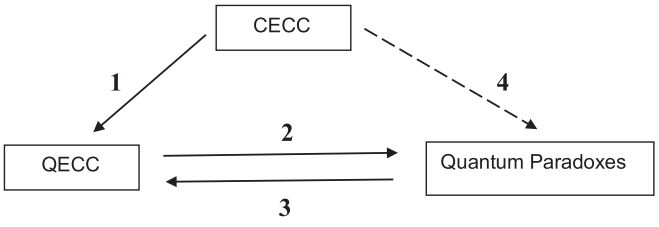

FIG. 1. CECC = Classical error correcting codes, QECC = Quantum error correcting codes, and Quantum paradoxes = Bell and KS theorems. The connection indicated by arrow 1 was made in many ways, notably by Steane [15] in his seven-qubit code and later in the CSS codes [17]. The connection 3 was made by Shor [7], who showed how the GHZ-Mermin proof could be made to yield quantum codewords, while several examples of the reverse connection 2 were pointed out by DiVincenzo and Peres [8]. The connection 4 was made in this paper, with the dashed arrow being used because we are aware of only two instances of it (based on the binary and ternary Golay codes).

One possible candidate of this kind is the binary quadratic residue code **[48,24,12]** whose generator matrix is given in [29]. This code has many words that differ from each other in exactly half their digits, and thus form pairs of orthogonal rays, but we have not been able to pick out a complete basis from them. If we could only do this,[9] we would have a KS proof. It would be nice to settle this issue one way or another and also identify other binary codes that might provide such proofs. The extension of this construction to ternary and n-ary codes is far from obvious.

Preskill [4] pointed out that the binary Golay code can be converted into a quantum error-correcting code via the CSS construction. Paralleling this, Prakash [30] recently demonstrated that the ternary Golay code can be converted into a 11-qutrit quantum error-correcting code that is useful for magic state distillation and fault-tolerant quantum computing. These applications of the Golay codes to current problems in quantum computing may lend some interest to the results of this paper, which show how the Golay codes can be used, with only a slight modification of their original form, to address a challenge that arose much earlier in the history of quantum mechanics.

If one notes that $12 = 2^2 3$, $24 = 2^3 3$, and $48 = 2^4 3$, these dimensions are the natural successors to $3 = 2^0 3$ and $6 = 2^1 3$. Dimension 3 is interesting because it is the lowest dimension in which the KS theorem holds and dimension 6 has the distinction of being the one in which the most compact KS proof (in terms of the number of contexts) is known [31]. Lisoněk [32] used a generalization of complex Hadamard

[8]Recall that the addition must be done by converting the rays into codewords and adding them bitwise modulo 2.

[9]Our problem is that we do not know any way, aside from tedious computation, of picking out a basis from the generator matrix of a linear code. We would certainly welcome any help or advice on this point.

matrices to show how the construction in [31] could be extended to many even dimensions, including the cases of 12 and 24 studied in this paper. However, his approach leads to KS sets in the complex spaces $\mathbb{CP}^{23}$ and $\mathbb{CP}^{11}$ that are not directly related to the KS sets found here, although they have the potential to be much smaller. It would be interesting to carry out a comparative study of the KS sets in the two approaches and see, in particular, which can be pushed to yield the smallest sets in dimensions 12 and 24.

An important feature of the Golay codes is their large symmetry group, which are Mathieu groups [2–4]. This symmetry is largely inherited by the system of rays and bases in which we looked for KS sets. Our past experience with highly symmetrical systems (in dimensions of the form 2^n) showed that they possess a large number of KS proofs with a rich and varied taxonomy.[10] It would be interesting to see if these features persist in the proofs obtained from the Golay codes.

Our proofs based on the Golay codes emerged after we first looked for such proofs in the Leech lattice, but gave up. To understand why the Leech lattice might be a good place to look, recall that the only dimensions in which the optimum dense packing of spheres is known are 8 and 24. In 8 dimensions the optimal packing is provided by the E8 lattice, and the 240 vectors from any lattice point to its nearest neighbors yield a system of 120 rays in $\mathbb{RP}^7$ that give rise to an astronomical number of KS proofs [34,35]. This led us to expect, by analogy, that the 196 560 vectors from a point of the Leech lattice to its nearest neighbors would give rise to a similarly large number of KS proofs. An investigation showed that this system possesses an extremely large number of bases, but the sheer size of the problem and the absence of any intuition of how to go about looking for KS proofs made us abandon it. However, we feel that a properly designed attack on the Leech lattice, perhaps based on graph theoretical techniques like those in [36] or [23], could reveal interesting information about the contextuality buried in it.

Finally, since many sporadic groups grew out of the Golay code and the Leech lattice, it is tempting to speculate that they might also be a fertile breeding ground for quantum contextuality in the high-dimensional spaces in which they operate.

[10]KS proofs derived from the 600-cell [33] and Gosset's eight-dimensional polytope [34] have just these features.

[1] M. Golay, Notes on digital coding, Proc IRE **37**, 657 (1949).

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups* (Springer-Verlag, New York, 1999).

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes* (North-Holland Elsevier, Amsterdam, 1983).

[4] J. Preskill, Lecture Notes for PH219/CS219, Chap. 7 Quantum Error Correction, available at http://theory.caltech.edu/~preskill/ph219/index.html. This chapter contains a discussion of the binary Golay code as well as its symmetry group.

[5] J. Leech, Notes on sphere packings, Canad. J. Math. **19**, 251 (1967).

[6] For a very accessible review of the sphere packing problem in higher dimensions, including the interesting cases of 8 and 24 dimensions, see H. Cohn, A conceptual breakthrough in sphere packing, Notices Amer. Math. Soc. **64**, 102 (2017).

[7] P. W. Shor, Scheme for reducing decoherence in quantum computer memory Phys. Rev. A **52**, R2493 (1995).

[8] D. P. DiVincenzo and A. Peres, Quantum code words contradict local realism, Phys. Rev. A **55**, 4089 (1997).

[9] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).

[10] R. Laflamme, C. Miquel, J. P. Paz and W. H. Zurek, Perfect Quantum Error Correcting Code, Phys. Rev. Lett. **77**, 198 (1996).

[11] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, Physics **1**, 195 (1964).

[12] S. Kochen and E. P. Specker, The problem of hidden variables in quantum mechanics, J. Math. Mech. **17**, 59 (1967); J. S. Bell, On the problem of hidden variables in quantum mechanics, Rev. Mod. Phys. **38**, 447 (1966).

[13] D. M. Greenberger, M. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos, (Kluwer, Dordrecht, The Netherlands, 1989), p. 69.

[14] N. D. Mermin, Hidden variables and the two theorems of John Bell, Rev. Mod. Phys. **65**, 803 (1993).

[15] A. M. Steane, Error Correcting Codes in Quantum Theory, Phys. Rev. Lett. **77**, 793 (1996).

[16] C. Budroni, A. Cabello, O. Guhne, M. Kleinmann and J.-A. Larsson, Quantum contextuality, arXiv:2102.13036v2; See Sec. III for many examples of the Kochen-Specker sets that were obtained in various dimensions.

[17] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A **54**, 1098 (1996).

[18] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, The Netherlands, 1993).

[19] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.106.062421 for a listing of the 220 rays corresponding to the codewords of weight 9, along with the 495 bases formed by them.

[20] For a more systematic approach to generating KS sets in various even dimensions using rays with components from a variety of number fields, see M. Pavičić and N. D. Megill, Vector generation of quantum contextual sets in even dimensional Hilbert spaces, Entropy **20**, 928 (2018).

[21] D. Meyer, Finite Precision Measurement Nullifies the Kochen-Specker Theorem, Phys. Rev. Lett. **83**, 3751 (1999); R. Clifton and A. Kent, Simulating quantum mechanics by non-contextual hidden variables, Proc. R. Soc. Lond. A **456**, 2101 (2000); J. Barrett and A. Kent, Non-contextuality, finite precision measurement and the Kochen-Specker theorem, Stud. Hist. Philos. Sci. **B 35**, 151 (2004).

[22] A. A. Klyachko, M. A. Can, S. Binicioglu, and A. S. Shumovsky, Simple Tests for Hidden Variables in Spin-1 Systems, Phys. Rev. Lett. **101**, 020403 (2008); S. Yu and C. H.

Oh, State-Independent Proof of Kochen-Specker Theorem with 13 Rays, *ibid.* **108**, 030402 (2012); M. Kleinmann, C. Budroni, J.-A. Larsson, O. Guhne, and A. Cabello, Optimal Inequalities for State-Independent Contextuality, *ibid.* **109**, 250402 (2012); A. Acín, T. Fritz, A. Leverrier, and A. B. Sainz, A combinatorial approach to nonlocality and contextuality, Commun. Math. Phys. **334**, 533 (2015).

[23] A. Cabello, S. Severini, and A. Winter, Graph-Theoretic Approach to Quantum Correlations, Phys. Rev. Lett. **112**, 040401 (2014).

[24] R. W. Spekkens, Contextuality for preparations, transformations, and unsharp measurements, Phys. Rev. A **71**, 052108 (2005); D. Schmid and R. W. Spekkens, Contextual Advantage for State Discrimination, Phys. Rev. X **8**, 011015 (2018); R. W. Spekkens, The ontological identity of empirical indiscernibles: Leibniz's methodological principle and its significance in the work of Einstein, arXiv:1909.04628.

[25] C. Simon, M. Żukowski, H. Weinfurter, and A. Zeilinger, Feasible Kochen-Specker Experiment with Single Particles, Phys. Rev. Lett. **85**, 1783 (2000); E. Amselem, M. Rådmark, M. Bourennane, and A. Cabello, State-Independent Quantum Contextuality with Single Photons, *ibid.* **103**, 160405 (2009); H. Bartosik, J. Klepp, C. Schmitzer, S. Sponar, A. Cabello, H. Rauch, and Y. Hasegawa, Experimental Test of Quantum Contextuality in Neutron Interferometry, *ibid.* **103**, 040403 (2009).

[26] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Contextuality supplies the "magic" for quantum computation, Nature (London) **510**, 351 (2014); S. Bravyi, D. Gosset, R. Konig, and M. Tomamichel, Quantum advantage with noisy shallow circuits, Nat. Phys. **16**, 1040 (2020).

[27] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography Against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007); K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, M. Pawlowski, and M. Bourennane, Contextuality offers device-independent security, arXiv:1006.0468.

[28] A. A. Abbott, C. S. Calude, J. Conder, and K. Svozil, Strong Kochen-Specker theorem and incomputability of quantum randomness, Phys. Rev. A **86**, 062109 (2012); A. A. Abbott, C. S. Calude, M. J. Dinneen, and N. Huang, Experimentally probing the algorithmic randomness and incompatibility of quantum randomness, Phys. Scr. **94**, 045103 (2019); A. Kulikov, M. Jerger, A. Potocnik, A. Wallraff, and A. Fedorov, Realization of a Quantum Random Generator Certified with the Kochen-Specker Theorem, Phys. Rev. Lett. **119**, 240501 (2017).

[29] M. Esmaeili, T. A. Gulliver, and A. K. Khandani, On the Pless-construction and ML decoding of the (48, 24, 12) quadratic residue code, IEEE Trans. Inf. Theory **49**, 1527 (2003).

[30] S. Prakash, Magic state distillation with the ternary Golay code, Proc. R. Soc. A. **476**, 20200187 (2020).

[31] P. Lisoněk, P. Badziąg, J. R. Portillo, and A. Cabello, Kochen-Specker sets with seven contexts, Phys. Rev. A **89**, 042101 (2014).

[32] P. Lisoněk, Kochen-Specker sets and complex Hadamard matrices, Theor. Comput. Sci. **800**, 142 (2019); This paper generalizes the construction described in Ref. [31] to certain higher dimensions by the use of a family of generalized complex Hadamard matrices.

[33] M. Waegell, P. K. Aravind, N. D. Megill, and M. Pavičić, Parity proofs of the Bell-Kochen-Specker theorem based on the 600-cell, Found. Phys. **41**, 883 (2011).

[34] M. Waegell and P. K. Aravind, Parity proofs of the Kochen-Specker theorem based on the Lie algebra E8, J. Phys. A: Math. Theor. **48**, 225301 (2015).

[35] P. Lisoněk, R. Raussendorf, and V. Singh, Generalized parity proofs of the Kochen-Specker theorem, arXiv:1401.3035v1; This paper describes a method for calculating the number of parity proofs in highly symmetrical systems. For the systems discussed in Refs. [33,34], it finds 2^{33} and 2^{1940} parity proofs, respectively. However, many of the proofs are contained within others in the count and only if distinct proofs are counted the total number is much smaller but still definitely in the astronomical range.

[36] R. Ramanathan, M. Rosicka, K. Horodecki, S. Pironio, M. Horodecki, and P. Horodecki, Gadget structures in proofs of the Kochen-Specker theorem, Quantum **4**, 308 (2020).