Kochen-Specker sets and Hadamard matrices

Petr Lisoněk
Department of Mathematics
Simon Fraser University
Burnaby, BC, V5A 1S6
Canada
plisonek@sfu.ca

July 31, 2018

Abstract

We introduce a new class of complex Hadamard matrices which have not been studied previously. We use these matrices to construct a new infinite family of parity proofs of the Kochen-Specker theorem. We show that the recently discovered simple parity proof of the Kochen-Specker theorem is the initial member of this infinite family.

1 Introduction

Kochen-Specker theorem is an important result in quantum mechanics [6]. It demonstrates the contextuality of quantum mechanics, which is one of its properties that may become crucial in quantum information theory [5]. In this paper we focus on proofs of Kochen-Specker theorem that are given by showing that, for \( n \geq 3 \), there does not exist a function \( f : \mathbb{C}^n \to \{0, 1\} \) such that for every orthogonal basis \( B \) of \( \mathbb{C}^n \) there exists exactly one vector \( x \in B \) such that \( f(x) = 1 \) (where \( \mathbb{C}^n \) denotes the \( n \)-dimensional vector space over the field of complex numbers). This particular approach has been used in many publications, see for example [1, 9, 10, 11] and many references cited therein. The following definition formalizes one common way of constructing such proofs.

\*Research was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC).
Definition 1.1. We say that $(\mathcal{V}, \mathcal{B})$ is a Kochen-Specker pair in $\mathbb{C}^n$ if it meets the following conditions:

1. $\mathcal{V}$ is a finite set of vectors in $\mathbb{C}^n$.
2. $\mathcal{B} = (B_1, \ldots, B_k)$ where $k$ is odd, and for all $i = 1, \ldots, k$ we have that $B_i$ is an orthogonal basis of $\mathbb{C}^n$ and $B_i \subset \mathcal{V}$.
3. For each $v \in \mathcal{V}$ the number of $i$ such that $v \in B_i$ is even.

Let us show that the existence of a Kochen-Specker pair demonstrates the non-existence of a function $f$ with the properties given above. Towards a contradiction suppose that $(\mathcal{V}, \mathcal{B})$ satisfies Definition 1.1 and $f : \mathbb{C}^n \to \{0, 1\}$ has the properties specified above. Denote $V_1 = \{x \in \mathcal{V} : f(x) = 1\}$. By conditions (2) and (3) and by properties of $f$, the number of $i$ such that $|B_i \cap V_1| = 1$ is even. Since the length of the list $\mathcal{B}$ is odd, there exists an $i$ such that $|B_i \cap V_1| \neq 1$, in contradiction to the required properties of $f$. Since this contradiction is based on a parity argument, the Kochen-Specker pairs introduced in Definition 1.1 are often called “parity proofs of the Kochen-Specker theorem.”

It is quite common in the literature [2, 9, 11] to refer to a Kochen-Specker pair as Kochen-Specker set, and we will do so sometimes in this paper. Kochen-Specker sets are key tools for proving some fundamental results in quantum theory and they also have various potential applications in quantum information processing [2]. In Section 3 we give a construction of a family of Kochen-Specker sets in infinitely many different dimensions. Before that, in Section 2 we introduce a new class of complex Hadamard matrices, which are used in our construction, and they may be also an interesting object of study on their own. In Section 4 we draw some conclusions from our results.

2 S-Hadamard matrices

For $z \in \mathbb{C}$ let $\overline{z}$ denote its complex conjugate. We work with the usual inner product on $\mathbb{C}^n$ defined by $\langle x, y \rangle = \sum_{i=1}^{n} x_i \overline{y_i}$. For a complex matrix $H$, let $H^*$ denote its conjugate transpose. Let $I_n$ denote the $n \times n$ identity matrix. We say that a complex number $z$ is unimodular if $|z| = 1$. We say that a vector $x \in \mathbb{C}^n$ is unimodular if each coordinate of $x$ is unimodular.

Definition 2.1. An $n \times n$ matrix $H = (h_{i,j})$ whose entries are complex numbers is called S-Hadamard matrix of order $n$ if it meets the following conditions:
(1) \[ HH^* = nI_n \]

(2) \[ |h_{i,j}| = 1 \text{ for all } 1 \leq i, j \leq n \]

(3) for each \( 1 \leq k, \ell \leq n, k \neq \ell \), we have \( \sum_{j=1}^{n} h_{k,j}^2 h_{\ell,j}^2 = 0 \).

Conditions (1) and (2) are the definition of Hadamard matrices which are prominent objects in combinatorial design theory that have been studied since the 19th century [4], first as matrices over \( \{ -1, 1 \} \) and then more generally as matrices over complex numbers. Condition (3) appears to be a new condition not previously seen in the literature. The proposed name \textit{S-Hadamard matrix} reflects the form of this new condition, which involves squares of the entries of \( H \). All three conditions in Definition 2.1 are required for our construction of Kochen-Specker pairs given in Theorem 3.1.

Throughout this paper we use additive notation for group operations. By \( \mathbb{Z}_g \) we denote the cyclic group of integers modulo \( g \).

**Definition 2.2.** [8, Definition 5.1] Let \( G \) be a group of order \( g \) and let \( \lambda \) be a positive integer. A \textit{generalized Hadamard matrix} over \( G \) is a \( g\lambda \times g\lambda \) matrix \( M = (m_{i,j}) \) whose entries are elements of \( G \) and for each \( 1 \leq k < \ell \leq g\lambda \), each element of \( G \) occurs exactly \( \lambda \) times among the differences \( m_{k,j} - m_{\ell,j} \), \( 1 \leq j \leq g\lambda \). Such matrix is denoted \( \text{GH}(g, \lambda) \).

**Proposition 2.3.** Suppose that \( g > 2 \) and \( \text{GH}(g, \lambda) \) over \( \mathbb{Z}_g \) exists. Then there exists an \( S \)-Hadamard matrix of order \( g\lambda \).

**Proof.** Assume that \( M = (m_{i,j}) \) is a \( \text{GH}(g, \lambda) \) over \( \mathbb{Z}_g \). Let \( \zeta_g = e^{2\pi\sqrt{-1}/g} \) be the primitive \( g \)-th root of unity in \( \mathbb{C} \). Define the \( g\lambda \times g\lambda \) matrix \( H = (h_{i,j}) \) by \( h_{i,j} = \zeta_g^{m_{i,j}} \) for all \( i, j \). We claim that \( H \) is an \( S \)-Hadamard matrix of order \( g\lambda \). We will verify that the three conditions in Definition 2.1 are satisfied. Let \( h_k \) and \( h_\ell \) be two rows of \( H \), \( k \neq \ell \). Then

\[
\langle h_k, h_\ell \rangle = \sum_{j=1}^{g\lambda} \zeta_g^{m_{k,j} - m_{\ell,j}} = \lambda \sum_{i=0}^{g-1} \zeta_g^i = 0
\]

and \( \langle h_k, h_k \rangle = \sum_{j=1}^{g\lambda} |h_{k,j}|^2 = g\lambda \), thus condition (1) is satisfied. Condition (2) follows from the construction of \( H \). To verify condition (3) we compute

\[
\sum_{j=1}^{g\lambda} h_{k,j}^2 h_{\ell,j}^2 = \sum_{j=1}^{g\lambda} \zeta_g^{2(m_{k,j} - m_{\ell,j})} = \lambda \sum_{i=0}^{g-1} \zeta_g^{2i} = \lambda \frac{\zeta_g^{2g} - 1}{\zeta_g^2 - 1} = 0
\]

where we used the assumption that \( g > 2 \), hence \( \zeta_g^2 \neq 1 \).
It would be interesting to find other constructions of S-Hadamard matrices, and we pose this as an open problem.

Example 2.4. The construction given in our main result (Theorem 3.1) requires the existence an S-Hadamard matrix of even order. For illustration let us consider small even orders. Proposition 2.3 allows one to construct an S-Hadamard matrix of order \( n \) for all even 0 \( < n \leq 100 \) except \( n = 2, 4, 8, 32, 40, 42, 60, 64, 66, 70, 78, 84, 88 \). The underlying generalized Hadamard matrices are obtained by constructions given in [8], moreover for \( n = 16 \) examples of GH(4,4) over \( \mathbb{Z}_4 \) are given in [3]. By consulting Table 6.1 in [7] we see that no other suitable GH(\( g, \lambda \)) over \( \mathbb{Z}_g \) are known for \( g \leq 7 \) and \( \lambda \leq 10 \). For some of the values of \( n \) which we excluded above, the existence of a suitable generalized Hadamard matrix is an open problem, and it is possible that S-Hadamard matrices of those orders may exist.

3 An infinite family of Kochen-Specker sets

S-Hadamard matrices introduced in the previous section will now be used to construct an infinite family of Kochen-Specker sets.

Theorem 3.1. Suppose that there exists an S-Hadamard matrix of order \( n \) where \( n \) is even. Then there exists a Kochen-Specker pair \((\mathcal{V}, \mathcal{B})\) in \( \mathbb{C}^n \) such that \( |\mathcal{V}| \leq \binom{n+1}{2} \) and \( |\mathcal{B}| = n + 1 \).

Proof. First we construct the set \( \mathcal{V} \). Let the elements of \( \mathcal{V} \) be denoted \( v^{\{r,s\}} \) where \( 1 \leq r, s \leq n + 1, r \neq s \). Note that we use the standard convention that sets are unordered, hence \( v^{\{r,s\}} \) and \( v^{\{s,r\}} \) denote the same element of \( \mathcal{V} \), for all \( r \neq s \). For \( x, y \in \mathbb{C}^n \) we define \( x \circ y = (x_1y_1, \ldots, x_ny_n) \).

Let \( H = (h_{i,j}) \) be the S-Hadamard matrix of order \( n \) whose existence is assumed, and let \( h_i \) denote the \( i \)-th row of \( H \). Without loss of generality we can assume that \( h_1 \) is the all-one vector, denoted \( \mathbf{1} \). If this is not the case, then replace each entry \( h_{ij} \) of \( H \) with \( h_{ij}h_{1j}^{-1} \); this operation preserves all conditions of Definition 2.1

We construct the elements of \( \mathcal{V} \) as follows:

- For \( 1 < s \leq n + 1 \) let \( v^{\{1,s\}} = h_{s-1} \).
- For \( 2 < s \leq n + 1 \) let \( v^{\{2,s\}} = h_{s-1} \circ h_{s-1} \).
- For \( 2 < r < s \leq n + 1 \) let \( v^{\{r,s\}} = h_{r-1} \circ h_{s-1} \).
For $1 \leq r \leq n + 1$ let $B_r = \{ v^{(r,i)} : 1 \leq i \leq n + 1, \ i \neq r \}$, and let $B = (B_1, \ldots, B_{n+1})$. We will now prove that each $B_r$ is an orthogonal basis of $\mathbb{C}^n$. Note that for $x, y, z \in \mathbb{C}^n$ such that $z$ is unimodular we have
\[
\langle z \circ x, z \circ y \rangle = \langle x \circ z, y \circ z \rangle = \sum_{i=1}^{n} x_i z_i y_i z_i = \langle x, y \rangle.
\] (1)

Since distinct rows of $H$ are orthogonal and all rows of $H$ are unimodular, equation (1) proves
\[
\langle v^{(r,s)}, v^{(r,t)} \rangle = \langle h_{r-1} \circ h_{s-1}, h_{r-1} \circ h_{t-1} \rangle = \langle h_{s-1}, h_{t-1} \rangle = 0
\]
whenever
\[
2 < r, s, t \leq n + 1 \quad \text{and} \quad r, s, t \text{ are distinct.} \tag{2}
\]

We will now prove the desired orthogonality relations $\langle v^{(r,s)}, v^{(r,t)} \rangle = 0$ for those pairs of vectors $v^{(r,s)}, v^{(r,t)}$ which are not covered by condition (2).

We will split the proof into cases according to the value of $r$.

Let $r = 1$. For $1 < s < t \leq n + 1$ we have
\[
\langle v^{(1,s)}, v^{(1,t)} \rangle = \langle h_{s-1}, h_{t-1} \rangle = 0.
\]

Now let $r = 2$. For $2 < s < t \leq n + 1$ we have
\[
\langle v^{(2,s)}, v^{(2,t)} \rangle = \langle h_{s-1} \circ h_{s-1}, h_{t-1} \circ h_{t-1} \rangle = \sum_{j=1}^{n} h_{s-1,j}^2 h_{t-1,j}^2 = 0
\]
by condition (3) in Definition 2.1. For $2 < t \leq n + 1$ we have
\[
\langle v^{(2,1)}, v^{(2,t)} \rangle = \langle 1, h_{t-1} \circ h_{t-1} \rangle = \sum_{j=1}^{n} h_{t-1,j}^2 = 0
\]
by condition (3) in Definition 2.1 applied with $k = 1$.

Now let $2 < r \leq n + 1$. For $t > 2, t \neq r$ we have
\[
\langle v^{(r,1)}, v^{(r,t)} \rangle = \langle h_{r-1} \circ h_{r-1} \circ h_{t-1} \rangle = \langle h_{r-1} \circ h_{1}, h_{r-1} \circ h_{t-1} \rangle = \langle h_{1}, h_{t-1} \rangle = 0
\]
as well as
\[
\langle v^{(r,2)}, v^{(r,t)} \rangle = \langle h_{r-1} \circ h_{r-1}, h_{r-1} \circ h_{t-1} \rangle = \langle h_{r-1}, h_{t-1} \rangle = 0.
\]
Finally we have
\[ \langle v^{(r,1)}, v^{(r,2)} \rangle = \langle h_{r-1}, h_{r-1} \circ h_{r-1} \rangle = \langle h_1 \circ h_{r-1}, h_{r-1} \circ h_{r-1} \rangle = \langle h_1, h_{r-1} \rangle = 0. \]

We note that \(|\mathcal{B}| = n + 1\) is odd since \(n\) is assumed to be even. We will complete the proof by verifying that condition (3) in Definition 1.1 is satisfied. If the mapping \(\{i,j\} \mapsto v^{(i,j)}\) is injective, then each \(v^{(i,j)}\) belongs to exactly two entries of \(\mathcal{B}\), namely \(B_i\) and \(B_j\). If the list \((v^{(i,j)})_{1 \leq i < j \leq n+1}\) contains repeated vectors, then let \(x\) be a vector that occurs exactly \(t\) times in this list. Then by the previous argument \(x\) belongs to exactly \(2t\) entries of \(\mathcal{B}\), since for distinct \(i, j, k\) we have \(v^{(i,j)} \neq v^{(i,k)}\) as \(\langle v^{(i,j)}, v^{(i,k)} \rangle = 0\). \(\square\)

There are infinitely many dimensions \(n\) to which Theorem 3.1 applies. By considering Proposition 2.3 a sufficient condition for applying Theorem 3.1 in an even dimension \(n\) is the existence of \(\text{GH}(g, n/g)\) over \(\mathbb{Z}_g\) for some \(g > 2\). The simplest forms of an infinite family for which this condition is satisfied are \(n = 2^k p^m\) where \(k \in \{1, 2\}\), \(p\) is an odd prime and \(m \geq 1\), or \(n = 8p\) where \(p > 19\) is prime. The constructions for the underlying generalized Hadamard matrices can be found by consulting Table 5.10 in [8]. Furthermore, any known generalized Hadamard matrices can be used as ingredients to recursive constructions given in Theorems 5.11 and 5.12 in [8]. As these recursive constructions can be applied repeatedly, it is impossible to give a closed form for all \(n\) to which Theorem 3.1 applies. For \(n \leq 100\) such \(n\) are listed in Example 2.4 above.

4 Conclusion

A Kochen-Specker pair \((\mathcal{V}, \mathcal{B})\) in \(\mathbb{C}^6\) with \(|\mathcal{V}| = 21\) and \(|\mathcal{B}| = 7\) was recently discovered [9]. It was noted [2] as the simplest Kochen-Specker pair (KS pair) since it strictly minimizes the cardinality of \(\mathcal{B}\) among all known KS pairs \((\mathcal{V}, \mathcal{B})\), see [11]. This KS pair was originally found by computer search and its internal structure has not been fully studied yet. In this paper we have revealed the structure of this KS pair, since it is obtained by applying Theorem 3.1 in the smallest possible dimension \(n = 6\). We have discovered an application of generalized Hadamard matrices to the construction of KS pairs, and we have proposed a new class of Hadamard matrices as the suitable domain for such constructions.
References

[1] A. Cabello, A proof with 18 vectors of the Bell-Kochen-Specker theorem. In: M. Ferrero and A. van der Merwe (Eds.), New Developments on Fundamental Problems in Quantum Physics. Kluwer Academic, Dordrecht, Holland, 1997, pp. 59–62.

[2] G. Cañas, M. Arias, S. Etcheverry, E.S. Gómez, A. Cabello, G.B. Xavier, G. Lima, Applying the simplest Kochen-Specker set for quantum information processing. Phys. Rev. Lett. 113 (2014), 090404.

[3] M. Harada, C. Lam, V.D. Tonchev, Symmetric (4,4)-nets and generalized Hadamard matrices over groups of order 4. Des. Codes Cryptogr. 34 (2005), 71–87.

[4] K.J. Horadam, Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ, 2007.

[5] M. Howard, J. Wallman, V. Veitch, J. Emerson, Contextuality supplies the ‘magic’ for quantum computation. Nature 510 (2014), 351–355.

[6] S. Kochen, E.P. Specker, The problem of hidden variables in quantum mechanics. Journal of Mathematics and Mechanics 17 (1967), 59–87.

[7] P.H.J. Lampio, Classification of difference matrices and complex Hadamard matrices. Dissertation, Aalto University, Helsinki, Finland, 2015. https://aaltodoc.aalto.fi/handle/123456789/18228 (Retrieved 30 November 2017)

[8] W. de Launey, Generalized Hadamard matrices. In: C.J. Colbourn and J.H. Dinitz (Eds.), Handbook of Combinatorial Designs. Second edition. Chapman & Hall/CRC, Boca Raton, FL, 2007, pp. 301–306.

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

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

[11] M. Waegell, P.K. Aravind, The minimum complexity of Kochen-Specker sets does not scale with dimension. Phys. Rev. A 95 (2017), 050101.