ARTICLE OPEN

Check for updates

Optimal measurement structures for contextuality applications

Yuan Liu[1], Ravishankar Ramanathan[1]✉, Karol Horodecki[2,3], Monika Rosicka[2] and Paweł Horodecki[3,4]

The Kochen-Specker (KS) theorem is a cornerstone result in the foundations of quantum mechanics describing the fundamental difference between quantum theory and classical non-contextual theories. Recently specific substructures termed 01-gadgets were shown to exist within KS proofs that capture the essential contradiction of the theorem. Here, we show these gadgets and their generalizations provide an optimal toolbox for contextuality applications including (i) constructing classical channels exhibiting entanglement-assisted advantage in zero-error communication, (ii) identifying large separations between quantum theory and binary generalized probabilistic theories, and (iii) finding optimal tests for contextuality-based semi-device-independent randomness generation. Furthermore, we introduce and study a generalization to definite prediction sets for more general logical propositions, that we term higher-order gadgets. We pinpoint the role these higher-order gadgets play in KS proofs by identifying these as induced subgraphs within KS graphs and showing how to construct proofs of state-independent contextuality using higher-order gadgets as building blocks. The constructions developed here may help in solving some of the remaining open problems regarding minimal proofs of the Kochen-Specker theorem.

npj Quantum Information (2023)9:63 ; https://doi.org/10.1038/s41534-023-00728-2

INTRODUCTION

The Kochen-Specker (KS) theorem[1,2] is a cornerstone result in the foundations of quantum mechanics, which delineates the differences between quantum theory and a class of hidden-variable theories obeying the principle of non-contextuality (NCHVTs). NCHVTs assume that outcomes are pre-assigned to measurements and independent of the particular contexts in which the measurements are realized. Informally, the KS theorem states that for every quantum system belonging to a Hilbert space of dimension d greater than two, irrespective of its actual state, a finite set of measurements exists whose results are logically impossible to be assigned of truth value 0 or 1 in a context-independent manner, satisfying (i) Exclusivity: two orthogonal projectors are not allowed to be both assigned 1, and (ii) Completeness: for each d mutually orthogonal projectors, one of them must be assigned 1.

KS sets are not the only means to identify the differences between quantum mechanics and NCHVTs. An interesting class of statistical state-dependent proofs of contextuality was also presented by Clifton[3], Stairs[4], Hardy[5] and others[6,7]. In these works, a prediction occurs with certainty in every non-contextual theory (such as the probability of an event being 0 or 1), while this is not the case in quantum theory. Such statistical proofs provide a simple and appealing contradiction between quantum and NCHVTs. Considering each projector in a Hilbert space as an atomic proposition, sets of the form $P \rightarrow \overline{Q}$ (P being true implies Q is false) or $P \rightarrow Q$ (P being true implies Q is true) have been termed as gadgets[7], definite-prediction sets[8], bugs or true-implies-false and true-implies-true sets[9].

As a central result in the foundations of quantum mechanics, KS contextuality has yielded several exciting applications in quantum information science recently. These applications include entanglement-assisted advantage in zero-error communication[10], semi-device-independent randomness generation[11], device-independent security[12], universal quantum computation via magic state distillation[13], advantage in communication complexity[14], self-testing quantum systems[15], etc.

In this paper, we introduce a general class of definite-prediction sets termed higher-order gadgets that goes beyond the basic 'true-implies-false' and 'true-implies-true' structures considered thus far and show how these gadget measurement structures provide an optimal toolbox for a plethora of applications of contextuality[12–14,16,17]. (i) We show how the entanglement-assisted advantage in zero-error communication, previously discovered for KS proofs alone, persists for the smaller and experimentally feasible classical channels corresponding to gadgets, under a suitable generalization. (ii) We apply gadgets to provide an experimentally feasible test of a recent result demonstrating that quantum correlations cannot be reproduced by fundamentally binary theories. These are a natural class of alternatives to the set of correlations allowed by quantum theory, and are defined as general probabilistic theories that posit that on a fundamental level only measurements with two outcomes exist. (iii) We point out that gadget-based contextuality tests allow to certify the maximal amount of $\log d$ bits of randomness from d-dimensional systems, making them ideal candidates for contextuality-based semi-device-independent randomness generation. (iv) We also use gadgets to point out a subtle modification to the famous Cabello-Severini-Winter (CSW) graph-theoretic framework of contextuality, namely that the classical value of non-contextuality inequalities does not always equal the weighted independence number of the corresponding orthogonality graph, when the KS rules of Exclusivity and Completeness are enforced. Furthermore, we show the constructions of definite prediction vector sets corresponding to arbitrary compound propositions, i.e., the entire spectrum of Hardy tests of contextuality from basic 'true-implies-false' sets to KS sets. We identify how these vector sets can be found inside general KS proofs, and demonstrate how

[1]Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong, Hong Kong. [2]Institute of Informatics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland. [3]International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland. [4]Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland. ✉email: ravi@cs.hku.hk

these can be applied as building blocks for constructing KS proofs as well as general state-independent contextual (SI-C) proofs. Consequently, since higher-order gadgets form an essential ingredient in the constructions of KS proofs, minimal constructions of gadgets may be expected to help resolve the long-standing open questions of minimal KS proofs in a given Hilbert space dimension.

RESULTS

Our results presented in this work are in two parts. On the one hand, as the fundamental results, we introduced the order (m, k) gadgets which play a crucial role in contextuality proofs. On the other hand, from the practical point of view, we proved that gadgets serve as the optimal measurement structures for several contextuality applications.

Order (m, k) gadgets and forbidden value assignments

In this work, we first introduced a general class of state-dependent contextuality proofs termed order (m, k) gadgets, which go beyond the known 01-gadgets[3–9]. An order (m, k) gadget contains m mutually non-orthogonal vectors with the property that at most k vectors among them can be assigned value 1 in any valid $\{0, 1\}$-assignment. In Hilbert space of dimension d, under some special constructions, we showed that when $m = d, k = d - 1$ an order (m, k) gadget can be constructed by any set of arbitrary non-orthogonal vectors $\{|v_1\rangle, \ldots, |v_m\rangle\}$. With this statement and construction, the Kochen-Specker (KS) sets as well as the general state-independent contextuality (SI-C) sets in dimension d can be constructed with the order $(k, k-1)$ gadgets as building blocks (for a fixed value k with $2 \le k \le d$). Apart from this, we also showed that order (m, k) gadgets form the building blocks of every KS proof by identifying them as induced subgraphs within any arbitrary KS proof.

We discussed a class of even more general measurement structures in which some specific $\{0, 1\}$-assignments are forbidden, a result that may be of independent interest and application. From this point of view, a 01-gadget is a set of vectors where the assignment $\{(1, 1)\}$ is forbidden on two given non-orthogonal vectors, an order (m, k) gadget is a set of vectors and for a given mutually non-orthogonal vectors subset $I = \{v_1, \ldots, v_m\}$ of it, the assignments of the form $\{(\underbrace{1, \ldots, 1}_{k+1}, f(v_{k+2}), \ldots, f(v_m)) \wedge (\textit{permutations})\}$ are forbidden (f is any $\{0, 1\}$-assignment function). And the KS sets are the ones that demonstrate the full forbidden value assignments $\{0, 1\}^{|I|}$ on any mutually non-orthogonal vectors subset I. A natural question then arises - can a gadget be constructed for every forbidden value assignment set? We answered this question in the affirmative and demonstrated the construction process in a concrete step-by-step manner.

Gadgets as optimal measurement structures to contextuality applications

Zero-error information theory is one of the most important applications of contextuality. Given a single use of a discrete, memoryless channel $\mathcal{N}$, the maximum number of (classical) messages that (a sender) Alice can send to (a receiver) Bob without causing any error is known as the one-shot zero-error capacity of $\mathcal{N}$. In groundbreaking work, Cubitt, Leung, Matthews and Winter[10] showed how to use KS proofs (specifically the KS graphs) to construct channels (confusability graphs) for which shared entanglement between Alice and Bob can increase the one-shot zero-error capacity. In analogy with them, we took the confusability graphs to be the orthogonality graphs of a certain class of gadgets and we considered a weighted version of the problem in which we assign weights w_i to the input symbols denoting the desirability of their transmission. It is in such a weighted version of the zero-error communication problem, we obtained an enhancement of the one-shot zero-error capacity via shared entanglement for channels corresponding to specific types of gadgets, which is a much wider class of graphs than was previously known.

While Quantum Theory is the most successful theory ever devised, there is still a huge research effort devoted to understanding physical and information-theoretic principles that force its formalism, one class of them is the Fundamentally Binary theories, these are no-signaling theories in which measurements yield many outcomes are constructed by selecting from binary measurements. Previously, the authors in[16,18] showed a Bell-type inequality to exclude the set of fundamentally binary non-signaling correlations as an underlying mechanism generating the set of quantum correlations, however, the proof is experimentally demanding since only small violations of the derived inequalities are possible, the violation of the derived inequality requires visibilities of $\approx 91.7\%$ of a suitably prepared two-qutrit state. We use the 01-gadget structures to derive the inequalities which are actually the maximum fractional assignments sum of the distinguished vectors, and from which the genuinely ternary character of quantum measurements can be certified in the much simpler single-system contextuality scenario with arbitrarily large separations between the set of quantum contextual correlations and the binary consistent correlations.

Contextuality can serve as the basis for randomness (or key) generation, and importantly one may utilize gadget-based contextuality tests to certify the optimal amount of randomness $\log_2 d$ per run which is the maximum randomness that can be extracted from a system of dimension d. To do that, in general one needs to derive a rigid contextuality test in dimension d and identify a suitable measurement x^* with fully random outcomes $P_{A|X}(a|x^*) = 1/d \; \forall \, a \in [d]$ when the maximum quantum value of the contextuality test is observed. We showed that the general constructions in[7] and the tunability of the overlap between the distinguished vectors of the gadgets make them ideal candidates for protocols allowing to certify the maximum amount of $\log_2 d$ bits of randomness. Specifically, we demonstrated the 01-gadgets in dimension $d = 4$ and 5 with the maximum overlaps between the distinguished vertices being $\frac{1}{\sqrt{d}}$ (for any orthogonal representation in $\mathbb{R}^d$), which indicate that one can readily derive contextuality tests allowing $\log_2 d$ bits optimal randomness certification from these constructions.

DISCUSSION

In this paper, we have introduced a generalization of gadget structures to definite prediction sets for arbitrary logical propositions and shown how gadgets are optimal measurement structures in many applications of contextuality. A number of interesting open questions remain. A fundamental question is to leverage the constructions of gadgets and their utility in building KS proofs to identify minimal KS proofs in a given dimension. It is still an open question to identify the minimal KS proof in dimension 3 while the 18-vector set introduced in[19,20] is conjectured to be minimal in dimension 4. With regard to applications, it is of interest to construct minimal gadget sets of measurements giving a contextuality test to certify the optimal amount of $\log d$ bits from a system of dimension d (constructions were shown for small dimensions here), and to use them in experimentally feasible contextuality-based randomness generation protocols. It is also of interest to experimentally test the separation between quantum mechanics and general binary consistent theories. In the future, it would be interesting to see if gadget generalizations can be used to show separations between quantum correlations and the set of n-ary consistent

correlations that are defined analogously to the binary theories as composed from measurements yielding at most n outcomes.

METHODS

Preliminaries

Much of the reasoning involving outcome contextuality has traditionally been carried out using graph-theoretic representations of KS sets, we therefore begin by establishing some graph-theoretic notation.

In this paper, we deal with simple, undirected, finite graphs $G = (V_G, E_G)$ where V_G and E_G denote the vertex and edge set of the graph respectively. If two vertices v_i, v_j are connected by an edge, we say that they are adjacent and denote it by $v_i \sim v_j$. A clique C in the graph G is a subset of vertices $C \subset V_G$ such that every pair of vertices in C is connected by an edge. A maximal clique is a clique that is not a subset of a larger clique, while a maximum clique in G is a clique of maximum size in G, we denote the size of the maximum clique by $\omega(G)$. An independent set in a graph G is a subset $I \subseteq V_G$ such that every pair of vertices in I is non-adjacent in G, the maximum size of an independent set is denoted $\alpha(G)$. A set of vertices $D \subset V_G$ is said to dominate a clique C if for every $v \in C$ there exists a $w \in D$ such that $\{v, w\} \in E$, that is every vertex of clique C has a neighbor in D. The set D is a minimal dominating set of C if no proper subset of D dominates C.

For any set of vectors $\mathcal{V}$, one can define an orthogonality graph $G_{\mathcal{V}}$ as the graph in which vector $|v\rangle \in \mathcal{V}$ is represented by a vertex v in $G_{\mathcal{V}}$ and two vertices v_1, v_2 are connected by an edge in $G_{\mathcal{V}}$ if and only if $\langle v_1|v_2\rangle = 0$[21]. Checking the orthogonality relations among the vectors from a given set $\mathcal{V}$ allows to efficiently establish its orthogonality graph $G_{\mathcal{V}}$. The problem of $\{0, 1\}$-coloring of a given set of vectors is then equivalently formulated as the problem of $\{0, 1\}$-coloring of its orthogonality graph defined in an analogous way as:

Definition 1. A $\{0, 1\}$-coloring of a graph G is a map $f: V_G \to \{0, 1\}$ such that (i) for every clique C in G, it holds that $\sum_{v \in C} f(v) \leq 1$, and (ii) for every clique C in G of size $\omega(G)$, there exists exactly one vertex $v \in C$ satisfying $f(v) = 1$.

The converse problem of identifying sets of vectors satisfying the orthogonality constraints dictated by the edges of a given graph is the question of finding an orthogonal representation of a graph.

Definition 2. An orthogonal representation of a graph G in dimension d is a set of (unit) vectors $\mathcal{S}$ from $\mathbb{C}^d$ such that there exists a map $f : V_G \mapsto \mathcal{S}$ satisfying the condition that $f(v_1)$ and $f(v_2)$ are orthogonal vectors if $\{v_1, v_2\} \in E_G$. The minimal dimension of an orthogonal representation of G is denoted $d(G)$. A faithful orthogonal representation of a graph G in dimension d is a set of (unit) vectors $\mathcal{S}$ from $\mathbb{C}^d$ such that there exists a map $f : V_G \mapsto \mathcal{S}$ satisfying the condition that $f(v_1)$ and $f(v_2)$ are orthogonal vectors if and only if $\{v_1, v_2\} \in E_G$, and furthermore $f(u)$ and $f(v)$ are non-parallel vectors if $u \neq v$. The minimal dimension of a faithful orthogonal representation of G is denoted $d^*(G)$.

We recall here the notion of 01-gadgets formalized in[7].

Definition 3. [7] A 01-gadget in dimension d is a {0,1}-colorable set $\mathcal{S}_{gad} \subset \mathbb{C}^d$ of vectors containing two distinguished non-orthogonal vectors $|u\rangle$ and $|v\rangle$ that nevertheless satisfy $f(u) + f(v) \leq 1$ in every {0,1}-coloring f of $\mathcal{S}_{gad}$.

Equivalently, the 01-gadgets may be defined in graph-theoretic terms as:

Definition 4. [7] A 01-gadget in dimension d is a {0,1}-colorable graph G_{gad} with faithful dimension $d^*(G_{gad}) = \omega(G_{gad}) = d$ and with two distinguished non-adjacent vertices u and v such that $f(u) + f(v) \leq 1$ in every {0,1}-coloring f of G_{gad}.

In other words, 01-gadgets are particular definite-prediction sets with a logical implication of the form $P \to \overline{Q}$, i.e., in any logical assignment of the set of atomic propositions, when one of the two distinguished propositions is assigned the value True the other is necessarily assigned value False, even though the distinguished atomic propositions are not represented by orthogonal vectors and are therefore not inherently exclusive to each other. In[7], it was shown that 01-gadgets identify the essential contradiction captured by the Kochen-Specker theorem, in that every KS graph contains a 01-gadget and from every 01-gadget one can construct a proof of the Kochen-Specker theorem (see also[22,23]). Note that by the famous Erdős-Stone theorem[24] of extremal graph theory, graphs of sufficiently high density necessarily contain subgraphs isomorphic to 01-gadgets, specifically the maximum number of edges in a graph (with faithful dimension d) with n vertices not containing a subgraph isomorphic to a 01-gadget (of dimension d) is $\left[\frac{d-2}{d-1} + o(1)\right]\binom{n}{2}$. This can be seen by observing that 01-gadgets in dimension d have chromatic number $\chi(G) = d$, where the chromatic number of a graph denotes the minimum number of colors needed to color the vertices such that adjacent vertices are assigned distinct colors.

From the preceding discussion, we recognize that the orthogonality graphs of Kochen-Specker vector sets do not admit a $\{0, 1\}$-coloring. The $\{0, 1\}$-colorability of a graph can also be formulated as an SAT instance and solved using a solver such as MiniSAT (http://minisat.se). To do this, one introduces a variable for each vertex in the graph. For each edge in the graph, a clause is added stating that the two incident vertices cannot both have value 1 (True). For each maximum clique in the graph, a clause is added stating that not all vertices in the clique have value 0 (False). The Boolean formulas for KS graphs are then seen to be unsatisfiable. Specifically, for the dimension $d = 3$ setting, one can formulate the $\{0, 1\}$-colorability of KS graphs as a 1-in-3 SAT instance. To do this, we complete the bases in the KS set by adding appropriate (unique) vectors, such that each edge in the graph belongs to a triangle. The Boolean formula in conjunctive normal form then has exactly three literals per clause, i.e., the formula is of the form $\wedge_{(i_1,i_2,i_3)\in \text{Cliques}}(v_{i_1} \vee v_{i_2} \vee v_{i_3})$ and the $\{0, 1\}$-colorability is equivalent to the 1-in-3 SAT question of determining whether there exists a truth assignment to the variables so that each clause has exactly one true literal. Furthermore, one can also obtain a similar unsatisfiable formula for 01-gadgets with an added clause stating that the two distinguished non-adjacent vertices both have value 1. Thus, from the point of view of satisfiability, 01-gadgets provide a similar (and in many cases, smaller) unsatisfiable instance. From the point of view of contextuality, 01-gadgets provide a state-dependent version of Kochen-Specker contextuality.

Order (m, k) gadgets

Let us now consider generalizations of gadget measurement structures that go beyond the basic 'true-implies-false' and 'true-implies-true' logical implications. Our first generalization is to gadgets of order (m, k) with $k \leq m$. Essentially, these are prediction sets corresponding to the proposition $\left[\left(\wedge_{i=1}^{k} P_i \to \wedge_{j=k+1}^{m} \overline{P}_j\right) \wedge (\textit{permutations})\right]$ for m mutually non-exclusive atomic propositions $P_1, \ldots, P_m$. In other words, the gadgets of order (m, k) contain m mutually non-orthogonal vectors such that at most k vectors can be assigned value 1 in any $\{0, 1\}$-coloring. The 01-gadgets[3,7,25–28] then correspond to the special case of gadgets of order (2, 1).

Definition 5. A gadget of order (m, k) in dimension d is a {0,1}-assignable set of vectors $\mathcal{S}_{m,k} \subset \mathbb{C}^d$ containing m distinguished mutually non-orthogonal vectors $\widetilde{\mathcal{S}}_{m,k} = \{|v_1\rangle, ..., |v_m\rangle\}\mathcal{S}_{m,k}$, such that

- for every subset $\mathcal{R} \subset \widetilde{\mathcal{S}}_{m,k}$ of size smaller than or equal to k, there exists a {0,1}-coloring which attributes 1 to all vectors in $\mathcal{R}$, and
- for any subset $\mathcal{R} \subset \widetilde{\mathcal{S}}_{m,k}$ of size greater than k, no {0, 1}-coloring exists that attributes 1 to all vectors in $\mathcal{R}$.

One can also give an equivalent definition of the order (m, k) gadget in graph-theoretic terms:

Definition 6. A gadget of order (m, k) in dimension d is a {0, 1}-colorable graph G with faithful dimension $d^*(G_{gad}) = \omega(G_{gad}) = d$ and with a distinguished independent set I of cardinality $|I| = m$ such that

- for every subset $I' \subset I$ of cardinality $|I'| \leq k$, there exists a {0, 1}-coloring of G in which all $v \in I'$ are assigned value 1, and
- no {0, 1}-coloring of G exists that assigns value 1 to more than k vertices from I.

We first study the question of whether a higher order (m, k) gadget can be constructed with any set of arbitrary vectors $\{|v_1\rangle, \ldots, |v_m\rangle\}$ as the distinguished vectors. While it is possible to consider every value of $k \in [m-1]$, here we focus on the construction for the special case $m = d, k = d-1$. As in the construction of KS sets, the construction of such general gadgets is complicated by the fact that even deciding the {0, 1}-colorability of a general graph is an NP-complete problem[29]. It is also hard in general to derive the faithful orthogonal representation of a graph in a given dimension. As such, there isn't a systematic method to derive minimal gadget structures. Nevertheless, we propose specific graphs G with candidate vertices to play the role of the distinguished vertices of the gadget. We then construct a symmetric matrix $\mathtt{Gram}$ with entries $\mathtt{Gram}_{i,j} = \mathtt{Gram}_{j,i} = 0$ corresponding to edges (i, j) in G. The matrix $\mathtt{Gram}$ is meant to represent the Gram matrix of a set of vectors realizing the graph G so that $\mathtt{Gram}_{i,j} = \langle v_i|v_j\rangle$. We study the question of finding a positive-semi-definite matrix completion $\mathtt{Gram} \geq 0$ with a rank-d constraint. We thus exhibit a graph that serves as an order $(d, d-1)$ gadget for arbitrary d, with the d distinguished vectors being $|m_1\rangle, |m_2\rangle, \cdots, |m_d\rangle$ (details are in the Supplementary Information Note 1). The feature of this construction is that the distinguished vectors can be chosen to be arbitrarily close to each other, i.e., $\langle m_i|m_j\rangle \to 1$ as the number of repeating units increases.

We now show an application of the higher-order gadgets in constructing KS proofs as well as general state-independent contextual (SI-C) proofs and also defer the details of these contractions to Supplementary Information Note 2.

Construction 1
Order $(k, k-1)$ gadgets can be used as building blocks to construct KS proofs in dimension d.

In the construction, we start with k bases $B_1, B_2, \ldots, B_k$ in dimension d, then randomly pick one vector in each basis to form a set $S_i = \left\{\left|v^q_{B_p}\right\rangle\right\}$ with $p \in [k] := \{1, \ldots, k\}$ and $q \in [d]$. In total, we have d^k such sets S_i. Then for each $i \in [d^k]$, we construct an order $(k, k-1)$ gadget in dimension d with the vectors in S_i being the distinguished vectors. Thus, assigning a single value 1 to each of the bases $B_1, \ldots, B_{k-1}$ forces all the vectors in the basis B_k to be assigned value 0 giving a contradiction, so that the union of all vectors is a KS proof.

Construction 2
Order $(k, k-1)$ gadgets can be used as building blocks to construct general SI-C sets in dimension d.

To realize the general SI-C set, we first construct a set of $r \cdot 2^n$ distinct unit vectors $|u_i\rangle$ in dimension d satisfying $\sum_{i=1}^{r\cdot 2^n} |u_i\rangle\langle u_i| = \frac{r\cdot 2^n}{d}\mathbb{1}_d$, where $r > \max\left\{\frac{d(k-1)}{2^n}, 4\right\}$ is an even integer and $n = \begin{cases} \lceil \log_2 \frac{d-1}{2} \rceil, & d \text{ is odd} \\ \lceil \log_2 \frac{d-2}{2} \rceil, & d \text{ is even} \end{cases}$. Then any k of these vectors form a set S_i, we first delete all the mutually orthogonal vectors in the set S_i and construct an order $(|S_i|, |S_i| - 1)$ gadget in dimension d with the vectors in S_i being the distinguished vectors. As a result, in any {0, 1}-assignment f, the sum of assignments of these $r \cdot 2^n$ vectors is smaller than k. On the other hand, in quantum theory we obtain the value $\frac{r\cdot 2^n}{d} > k$ for every state in dimension d, so that the union of all the vectors gives a proof of state-independent contextuality. Finally, not only can the higher-order gadgets be used as building blocks to construct KS proofs, we also show that specific such gadgets may be found as necessary substructures (induced subgraphs) in any proof of the KS theorem.

Theorem 1. Every KS set in dimension d contains a gadget of order $(k, k-1)$ for some k satisfying $2 \leq k \leq d$.

The intuition behind the proof is that if no {0, 1}-coloring exists for a graph G, a brute-force greedy algorithm that attempts to assign 0s and 1s to its vertices must stop at some point in its execution, before each maximum clique has a single 1-valued vertex. Therefore, there must exist some clique C in G such that each vertex in C is adjacent to some 1-valued vertex at this point in the execution. Call such a minimal set of adjacent vertices to a maximum clique as D, then the induced subgraph formed by $D \cup C$ constitutes a gadget. Furthermore, such a gadget must be of order at least $(k, k-1)$.

Order (m, k) gadgets are thus a natural generalization of 'True-implies-False' sets, where we consider an independent set $I = \{v_1, \ldots, v_m\}$ of vertices (mutually non-orthogonal vectors) with forbidden value assignments of the form $\{\underbrace{1, \ldots, 1}_{k+1}, f(v_{k+2}), \ldots, f(v_m)\}$ and permutations thereof, for any {0, 1}-coloring f. One may consider yet more general structures in which we specify a general set of forbidden value assignments $\mathcal{H} \subset \{0, 1\}^m$, we elaborate on this in Supplementary Information Note 3.

Entanglement-assisted advantage in Zero-error communication in channels constructed from gadgets

One of the most important and tantalizing applications of contextuality is in the field of zero-error information theory. In classical zero-error coding, we consider a discrete, memoryless channel $\mathcal{N}$ connecting a sender Alice and a receiver Bob. Given a single use of such a channel, the maximum number of classical messages that Alice can send to Bob under the constraint that there be no error is known as the one-shot zero-error capacity of $\mathcal{N}$. In groundbreaking work, Cubitt et al.[10] showed how to use KS proofs to construct channels for which shared entanglement between Alice and Bob can increase the one-shot zero-error capacity. Since 01-gadgets are substructures of KS proofs, it is an interesting question to investigate whether these smaller (and experimentally more feasible) measurement structures already exhibit the phenomenon of entanglement-assisted advantage in zero-error capacity.

The classical channel $\mathcal{N}$ has finite inputs X and outputs Y and its behavior is characterized by the probability distribution $\mathcal{N}_{Y|X}(y|x)$ of outputs given inputs. Two inputs x are confusable if the corresponding distributions on outputs overlap. The confusability graph $G(\mathcal{N})$ is constructed with vertex set being the set of input symbols and two vertices connected by an edge if the corresponding input symbols are confusable. A zero-error code is then a set of non-confusable inputs and the one-shot zero-error

capacity of the channel is the maximum size of such a set. When Alice and Bob only share correlations which can be obtained using shared randomness, this number can be readily seen to be the independence number of the graph $G(\mathcal{N})$, i.e., $c_{SR}(\mathcal{N}) = \alpha(G(\mathcal{N}))$ where $c_{SR}(\mathcal{N})$ denotes the zero-error capacity when using correlations obtained using shared randomness as a resource. On the other hand, Cubitt et al. showed examples of channels for which sharing entanglement can improve the zero-error capacity of sending classical messages, i.e., such that $c_{SE}(\mathcal{N}) > c_{SR}(\mathcal{N})$ where $c_{SE}(\mathcal{N})$ denotes the zero-error capacity when using shared entanglement as a resource. In particular, they showed that such channels arise naturally from proofs of the Kochen-Specker theorem, specifically one may take $G(\mathcal{N})$ to be the (non-{0, 1}-colorable) orthogonality graph of some Kochen-Specker vector set.

We show that one may also take $G(\mathcal{N})$ to be the orthogonality graph of a certain class of gadgets, by a suitable generalization to a weighted version of the zero-error communication problem. In the weighted generalization, we assign weights $w = \{w_i\}_{i=1}^{|V|}$ to the input symbols (denoting the desirability of their transmission). The one-shot zero-error capacity is then the maximum total weight of any set of non-confusable inputs, which corresponds to the weighted independence number of the confusability graph, i.e., $c_{SR}(\mathcal{N}, w) = \alpha(G(\mathcal{N}), w)$.

Consider a gadget in which we complete each of the bases (by addition of suitable vectors satisfying the orthogonality relations) such that a clique cover of the graph is possible in which the vertices of the graph are partitioned into q maximum cliques (of size $\omega(G) = d$) given as $C_m = \{v_{m,1}, \ldots, v_{m,d}\}$ for $m = 1, \ldots, q$ (i.e., $V = \cup_{m=1}^{q} C_m$). We remark that a similar completion is required for the graphs obtained from Kochen-Specker proofs in[10], and only such Kochen-Specker proofs (such as the Peres-Mermin proof[30] with 24 vectors partitioned into six cliques in dimension 4) display the enhancement proven there.

We construct the channel $\mathcal{N}$ as having inputs in $[q] \times [d]$ with inputs (m, i) and (m', i') being confusable if and only if the corresponding vectors are orthogonal to each other, i.e., if and only if $\langle v_{m,i} | v_{m',i'} \rangle = 0$. $G(\mathcal{N})$ has an edge between such pairs of confusable inputs and is exactly the orthogonality graph corresponding to the (base-completed) gadget. By construction, the vertices of $G(\mathcal{N})$ can be partitioned into q maximum cliques (of size d). We now consider the weighted version of the zero-error communication problem with V_{dist} denoting the set of distinguished vertices in the gadget as

$$w_i = \begin{cases} w^* & i \in V_{\text{dist}} \\ 1 & i \in V \setminus V_{\text{dist}} \end{cases} \tag{1}$$

for a parameter w^*. The one-shot zero-error capacity when only shared randomness is available is then readily calculated to be $c_{SR}(G(\mathcal{N})) = \max\{\alpha(G(\mathcal{N})) - 1 + w^*, \alpha(G(\mathcal{N})) - 3 + 2w^*\}$. We choose $w^* > 1$ such that $2w^* - 3 < w^* - 1$, i.e., $1 < w^* < 2$ giving $c_{SR}(G(\mathcal{N})) = \alpha(G(\mathcal{N})) - 1 + w^* < q + w^* - 1$.

On the other hand, suppose Alice and Bob share a maximally entangled state $|\psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i, i\rangle$. Each message m that Alice wishes to send corresponds to a maximum clique in the aforementioned clique partitioning of the graph $G(\mathcal{N})$. To send m, Alice measures in the bases given by the clique C_m and obtains an outcome $k \in [d]$ with probability $1/d$. Her input to the channel is then (m, k). The output of the channel at Bob's end is one of the maximum cliques containing the vertex $v_{m,k}$ (not necessarily belonging to the clique partitioning of the graph). Bob performs a projective measurement corresponding to his received maximum clique, and his outcome reveals Alice's input to the channel. The one-shot zero-error capacity when shared entanglement is used as a resource is then calculated to be $c_{SE}(G(\mathcal{N})) = \frac{1}{d}[qd - |V_{\text{dist}}| + |V_{\text{dist}}| \cdot w^*] = q + \frac{(w^*-1)|V_{\text{dist}}|}{d}$. We see that $c_{SE}(G(\mathcal{N})) > c_{SR}(G(\mathcal{N}))$ whenever $|V_{\text{dist}}| > d$, i.e., whenever we have a gadget-type graph with $|V_{\text{dist}}|$ distinguished vertices of which only one can be assigned value 1 in any non-contextual {0, 1} value assignment.

We note that such a gadget-type graph does not correspond to a Kochen-Specker proof since it is {0, 1}-colorable. On the other hand, one can construct a state-independent non-contextuality inequality for the graph that is violated by all states in dimension d, namely $\sum_{v_i \in V_{\text{dist}}} P(e_{v_i}) \leq 1$, where $P(e_i)$ refers to the probability of the event e_{v_i} corresponding to the distinguished vertex v_i. Such graphs may therefore be said to be of the type discovered by Yu and Oh in[31], namely they exhibit state-independent contextuality despite not corresponding to a Kochen-Specker proof. And as we have seen, we obtain an enhancement via entanglement of the one-shot zero-error capacity for all such graphs, a much wider (and easily constructible following the constructions in[7] and Construction 2 in this work) class of graphs than was previously known.

Large violations of binary consistent correlations in quantum theory

In this section, we describe an application of the gadget constructions to the task of excluding a natural alternative to quantum theory, namely the so-called "Fundamentally Binary theories"[16,18]. While Quantum Theory is the most successful theory ever devised, there is still a huge research effort devoted to understanding physical and information-theoretic principles that force its formalism. Seemingly natural alternatives to the set of correlations allowed by Quantum Theory exist such as the so-called 'Almost Quantum' correlation set[32]. Another class of natural alternatives is given by the Fundamentally Binary theories, these are no-signaling theories in which measurements yielding many outcomes are constructed by selecting from binary measurements. In other words, these theories posit that on a fundamental level only measurements with two outcomes exist, and scenarios where a measurement has more than two outcomes are achieved by classical post-processing of one or more two-outcome measurements. Fundamentally binary correlations are characterized as the convex hull of all consistent correlations $\{P(a|x)\}$ obeying the constraint that for all x, it holds that $P(a|x) = 0$ for all but two outcomes a.

In[16,18], it was shown that two-party non-locality scenarios exist such that the corresponding class of fundamentally binary non-signaling correlations does not fully encompass the set of quantum correlations. In other words, it was shown that a Bell-type inequality can be constructed to exclude the set of fundamentally binary non-signaling correlations as an underlying mechanism generating the set of quantum correlations. The authors of[16,18] considered the simplest non-trivial polytope of fundamentally binary non-signaling correlations involving two parties that perform two measurements with three outcomes each. They computed the facets of the polytope using Fourier-Motzkin elimination using the software `porta` and calculated the corresponding quantum violations using the NPA semidefinite programming hierarchy[33]. While an important foundational result, the proof in[18] is experimentally demanding in that only small violations of the derived inequalities are possible (the quantum value being $I_a = 2(2/3)^{3/2} \approx 1.0887$ compared to the value in binary theories of $I_a = 1$), the violation of the derived inequality requires visibilities of $\approx 91.7\%$ of a suitably prepared two-qutrit state. In this section, we show that the genuinely ternary character of quantum measurements can be certified in the much simpler single-system contextuality scenario with arbitrarily large separations between the set of quantum contextual correlations and the binary consistent correlations. The price to pay for such large violations is the assumption, common to all contextuality experiments, that the same projector is measured in different contexts.

Consider an orthogonality graph $G=(V_G,E_G)$ with a set of maximum cliques (contexts) $\mathcal{C}_\mathcal{G}=\{A_1,\ldots,A_k\}$ where each clique A_i is of size $\omega(G)=d$. A box $B=\{P(a|x)\}$ is a set of conditional probability distributions with input $x\in\{1,\ldots,k\}$ and output $a\in\{1,\ldots,d\}$. A box is said to be compatible with an orthogonality graph G if it is a family of (normalized) probability distributions such that for each $c\in\{A_1,\ldots,A_k\}$, there is a corresponding probability distribution in this family.

Definition 7. For a given orthogonality graph $G=(V_G,E_G)$ with a set of contexts $\mathcal{C}_G=\{A_1,\ldots,A_k\}$, a box $B=\{P(a|x)$ is said to be a Consistent Box if for all pairs $c,c'\in\mathcal{C}_G$ and for sets of vertices (projectors) $S_{c,c'}=c\cap c'\neq\emptyset$, it holds that

$$\forall s\in S_{c,c'}\quad P(a=s|x=c)=P(a=s|x=c'). \tag{2}$$

The set of all consistent boxes B compatible with an orthogonality graph G is denoted by B_G^c.

Note that the set of non-signaling boxes is a special case of such consistent boxes.

Fundamentally binary correlations are a sub-class of consistent correlations obtained as the convex hull of consistent boxes for which for each context c in the graph G (maximum clique of size $\omega(G)=d$) at most two projectors (vertices in the clique) are assigned non-zero values that sum to unity and the remaining projectors in the context are assigned value 0, together with any box obtained by local classical postprocessing of such boxes. Note that in each extremal binary consistent box, the assignment of values to the projectors is done in a consistent manner, so that the value assigned to any projector is independent of the context in which it is measured. Formally we define binary consistent correlations as follows.

Definition 8. For a given orthogonality graph $G=(V_G,E_G)$ with a set of contexts $\mathcal{C}_G=\{A_1,\ldots,A_k\}$, a binary consistent assignment is a function $f:V_G\to[0,1]$ such that $\forall c\in\mathcal{C}_G$, *exists* $v_1,v_2\in c$ such that $f(v_1)+f(v_2)=1$ and $f(v_i)=0$ for all $v_i\in c\setminus\{v_1,v_2\}$. Define the set of boxes $B_G^{\text{bin-cons}}$ as the convex hull of boxes obtained by binary consistent assignments, i.e.,

$$B_G^{\text{bin-cons}} := \text{conv}\,\{\{P(a|x)\}\in B_G^c \mid \forall c\in\mathcal{C}_G,\ \exists s_1,s_2\in c \ \text{s.t.}\ P(a=s_1|x=c)+P(a=s_2|x=c)=1\}. \tag{3}$$

The set of Fundamentally Binary boxes B_G^{bin} is defined as the set of boxes that can be obtained by local classical postprocessing from any $B\in B_G^{\text{bin-cons}}$.

We now show that not only does the set of Fundamentally Binary boxes not encompass the set of quantum contextual correlations, but that in fact there exist separating inequalities for which large violations by quantum contextual correlations can be obtained.

Theorem 2. There exist inequalities bounding the set of fundamentally binary consistent correlations that admit close to algebraic violations in quantum theory.

Proof. The proof will make use of the idea of 'extended 01-gadgets' that we introduced in[7].

Definition 9. An extended 01-gadget in dimension d is a $\{0,1\}$-colorable graph $G_{xgad}=(V_{xgad},E_{xgad})$ with faithful dimension $d^*(G_{xgad})=\omega(G_{xgad})=d$ and with two distinguished non-adjacent vertices $v_1\nsim v_2$ such that in any assignment $f:V_{xgad}\to[0,1]$, it holds that $f(v_1)+f(v_2)<2$.

In other words, an extended 01-gadget is similar to a normal 01-gadget except that the defining characteristic holds for arbitrary assignments in $[0,1]$ rather than only to $\{0,1\}$ assignments.

In[7], we had proven the following statement that shows a construction of an extended 01-gadget between any two non-orthogonal vectors in $\mathbb{C}^d$.

Lemma 1. (Theorem 4 in[7]). Let $|v_1\rangle$ and $|v_2\rangle$ be any two distinct non-orthogonal vectors in $\mathbb{C}^d$ with $d\geq 3$. Then there exists an orthogonality graph G_{xgad} that constitutes an extended 01-gadget in dimension d with the corresponding vertices v_1 and v_2 being the distinguished vertices.

We now show that for any extended 01-gadget, the sum of the binary consistent (probability) assignments to the two distinguished vertices in any box $B\in B_G^{\text{bin-cons}}$ is at most 3/2. To do so, we recall the notion of the Fractional Stable-Set Polytope ($FSTAB(G)$) of a graph $G=(V_G,E_g)$ which is defined as

$$FSTAB(G)=\left\{\vec{x}\in\mathbb{R}_+^{|V_G|}\mid x_v+x_w\leq 1\ \ \forall(v,w)\in E_G\right\}. \tag{4}$$

We recognize that the fractional stable-set polytope is defined by similar constraints to the set of binary boxes $B_G^{\text{bin-cons}}$ except for the fact that the defining constraint $x_v+x_w\leq 1$ in $FSTAB(G)$ is replaced by the constraint that $\forall c\in\mathcal{C}_G,\exists\, v,w\in c$ such that $x_v+x_w=1$ in $B_G^{\text{bin-cons}}$. By introducing a slack variable $y_{v,w}$ for each edge constraint, we rewrite the fractional stable-set polytope as

$$FSTAB(G)=\left\{(\vec{x},\vec{y})\in\mathbb{R}_+^{|V_G|}\times\mathbb{R}_+^{|E_G|}\mid x_v+x_w+y_{v,w}=1\ \ \forall(v,w)\in E_G\right\}. \tag{5}$$

Here, every vertex of G indexes an x variable while every edge of G indexes a slack y variable, so that x and y can be termed vertex variables and edge variables respectively. A vertex v is said to be k-valued in the fractional assignment $(\vec{x},\vec{y})$ if the corresponding vertex variable takes value k, and similarly an edge (v,w) is said to be j-valued in the assignment if the corresponding edge variable takes value j. The following theorem by Nemhauser and Trotter[34], following an earlier result by Balinski[35] provides a characterization of the vertices of $FSTAB(G)$.

Theorem 3. (Balinski[35], Nemhauser and Trotter[34]). Let $\vec{x}\in\mathbb{R}_+^{|V_G|}$ be a vertex of $FSTAB(G)$. Then for every vertex $v\in V_G$, it holds that $x_v\in\{0,\frac{1}{2},1\}$, i.e., that every vertex is 0 or 1/2 or 1-valued in $\vec{x}$.

Now, since the set of normalization conditions $NORM_G:=\{\text{NORM}_G^c\}_c$ for the maximum cliques $c\in\mathcal{C}_G$ where

$$\text{NORM}_G^c:=\{\exists v,w\in c\ \text{ s.t. }\ f(v)+f(w)=1\} \tag{6}$$

form supporting hyperplanes of $FSTAB(G)$, we see that the vertices of $FSTAB(G)\cap NORM_G$ inherit the characterization derived in the above theorem, i.e., the corresponding edge (slack) variables y take value 0 for each edge in the graph. We thus obtain

Corollary 1. Let $\{P(a|x)\}$ be a vertex of $B_G^{\text{bin-cons}}$. Then for every context $c\in\mathcal{C}_G$ and for every outcome $s\in[d]$, it holds that $P(a=s|x=c)\in\{0,\frac{1}{2},1\}$.

It is also worth remarking that classical processing does not change the above property so that it holds also for the extreme points of the polytope of Fundamentally Binary boxes B_G^{bin}. Applying the above corollary to any orthogonality graph G_{xgad} that constitutes an extended 01-gadget, we see that the sum of the binary consistent assignments to the two distinguished vertices is at most 3/2.

This statement, in conjunction with the constructions of extended 01-gadgets in the lemma for distinguished vectors $|v_1\rangle,|v_2\rangle$ satisfying $|\langle v_1|v_2\rangle|\to 1$ shows that the inequality $P(a=v_1|x=c_{v_1})+P(a=v_2|x=c_{v_2})\leq 3/2$ forms a supporting inequality

for $B^{\mathrm{bin}}_{G_{xgad}}$, where c_{v_1} and c_{v_2} are two contexts containing the vertices v_1 and v_2 respectively. On the other hand, measurements of the contexts on the state $|v\rangle = \frac{1}{\sqrt{2(1+\cos\theta)}}(|v_1\rangle + |v_2\rangle)$ with $\langle v_i|v_j\rangle = \cos\theta$ show that Quantum Theory achieves the value $(1+\cos\theta) \to 2$ as $\theta \to 0$.

It is worth remarking that separations between the sets of binary consistent correlations and quantum correlations are not achieved by considering the inequalities for the usual Kochen-Specker proofs since both sets achieve the algebraic value for those inequalities. This shows the importance of the constructions of gadgets and extended gadgets in deriving such separating hyperplanes. Furthermore, it is also clear that higher-order extended gadgets can be constructed in analogy with the constructions of higher-order gadgets in the rest of this paper. In the future, it would be interesting to see if these constructions can be used to show large separations between the set of quantum contextual correlations and the set of n-ary consistent correlations that are defined analogously to the binary consistent correlations as composed from measurements yielding at most n outcomes.

Optimal semi-device-independent randomness generation using gadgets

Contextuality can serve as the basis for randomness (or key) generation, either via stand-alone protocols that test for the violation of a non-contextuality inequality[11] (where one assumes that the measurements conform to the specific orthogonality graph), or through the conversion of a single-party contextuality test into a two-party Bell inequality[12] or through the conversion of a non-contextuality inequality to a prepare-and-measure protocol[14]. A common step in all such protocols[36–41] is the identification of a suitable measurement in the (contextuality) test that yields the highest possible randomness or key generation rate. It is well-known that the maximum randomness (quantified by the min-entropy) per run that can be extracted from a test where the parties perform projective measurements on a system of dimension d is $\log_2 d$. The importance and utility of gadgets for randomness certification have been commented on previously, we elaborate on this aspect and focus on their importance for optimal randomness certification in this section.

The Kochen-Specker theorem shows that it is impossible to assign classical (deterministic) values to all quantum observables in a consistent manner, i.e., independent of the context in which the observables are measured. However, as pointed out in[42,43], the fact that not all quantum observables can be assigned definite values does not imply that no observable can be assigned a definite outcome. And in general, proofs of contextuality do not specify which observables are value-indefinite. Specifically, for a contextuality test with a set of observables $\{A_1, \ldots, A_k\}$ we want to solve

$$\begin{aligned} &\max \quad P_{guess}(A_i|E) \\ &s.t. \quad I(P_{A|X}) = I^*, \\ &\qquad P_{A,E|X} \in \mathcal{Q}, \end{aligned} \tag{7}$$

where $I(P_{A|X})$ is a non-contextuality inequality evaluated on the observed conditional probability distributions $P_{A|X}$, $I^* \in (I_c, I_q]$ with classical and quantum values given by I_c and I_q respectively, and $\mathcal{Q}$ denotes the set of conditional distributions (boxes) achievable by performing measurements (compatible with the test structure on Alice's side) on quantum states shared between Alice and adversary Eve, $P_{guess}(A_i|E) = \sum_e P(e)P_e(a=e|i)$ is the guessing probability of Alice's outcome by an adversary E. By an optimal rigid contextuality test in dimension d we mean one in which there exists a measurement basis x^* such that $P_{A|X}(a|x^*) = 1/d$ for all outcomes $a \in [d]$ when the maximum value I_q is observed. It is an open question to derive such a rigid class of contextuality tests for arbitrary dimension d (see for example[14] where the guessing probability was calculated for the well-known 5-cycle non-contextuality inequality[44]).

Constructions of gadgets provide a candidate solution to the problem. Specifically, the extended 01-gadgets from Definition 9 were used in[7] as building blocks to construct sets of vectors $\mathcal{S}'$ such that for any $[0,1]$-assignment $f : \mathcal{S}' \to [0,1]$ it holds that $f(|v_1\rangle), f(|v_2\rangle) \in \{0,1\}$ if and only if $f(|v_1\rangle) = f(|v_2\rangle) = 0$. A first interesting aspect of these gadgets for randomness certification is that they allow to localize the randomness guaranteed by the KS theorem (note that a similar theorem with a more complicated construction was explored in[45]). In other words, the observation in the contextuality test of $P(|v_1\rangle) = 1$ guarantees that $0<P(|v_2\rangle)<1$ for any consistent box P compatible with the measurement structure of the gadget. Secondly, if one has a rigid construction[15] with overlap $|\langle v_1|v_2\rangle| = 1/\sqrt{d}$, one can readily derive a contextuality test allowing optimal randomness certification (for example with a non-contextuality inequality of the form $\beta P(|v_1\rangle) + P(|v_2\rangle) \leq \beta$ with $\beta \gg 1$, for which the optimal quantum value is then $\beta + 1/d$). Here, by a rigid construction we mean one for which there exists a non-contextuality inequality whose maximum violation certifies a fully random outcome (with uniform probabilities $1/d$) for one of the measurement bases in the construction. One way to ensure this is if for the construction, the set of vectors realizing its orthogonality graph G is unique in $\mathbb{C}^{\omega(G)}$ (up to unitaries). For the gadget-within-gadget construction in the proof of Theorem 4 in[7], it was shown that for the k-th iteration in the construction the maximum overlap of the distinguished vectors takes the form $\frac{k}{k+2}$, so that the construction allows optimal randomness certification for $d=4$ at $k=2$. As shown in Fig. 1, the maximum overlap between the distinguished vectors $|u_1^{(2)}\rangle, |u_8^{(2)}\rangle$ is $\frac{1}{2}$, and the orthogonal representation of this gadget is $\langle v_1^{(1)}| = \langle v_4^{(2)}| = (1,0,0)$, $\langle v_2^{(1)}| = (0, -\frac{\sqrt{3}}{2}, \frac{1}{2})$, $\langle v_3^{(1)}| = (0, \frac{\sqrt{3}}{2}, \frac{1}{2})$, $\langle v_4^{(1)}| = (-1, -\frac{\sqrt{2}}{2}, -\frac{\sqrt{6}}{2})$, $\langle v_5^{(1)}| = (-1, -\frac{\sqrt{2}}{2}, \frac{\sqrt{6}}{2})$, $\langle v_6^{(1)}| = (\frac{\sqrt{2}}{3}, -\frac{1}{6}, -\frac{\sqrt{3}}{6})$, $\langle v_7^{(1)}| = (\frac{\sqrt{2}}{3}, -\frac{1}{6}, \frac{\sqrt{3}}{6})$, $\langle v_8^{(1)}| = \langle v_5^{(2)}| = \frac{2\sqrt{2}}{3}(\frac{\sqrt{2}}{4}, 1, 0)$, $\langle v_1^{(2)}| = (-\frac{3}{2}, -\frac{3\sqrt{2}}{4}, \frac{3\sqrt{2}}{4})$, $\langle v_2^{(2)}| = (0,1,1)$, $\langle v_3^{(2)}| = (-\frac{3\sqrt{2}}{4}, \frac{3}{8}, -\frac{8}{9})$, $\langle v_6^{(2)}| = (0,-1,1)$, $\langle v_7^{(2)}| = (1, -\frac{\sqrt{2}}{4}, -\frac{3\sqrt{2}}{4})$ $\langle v_8^{(2)}| = (\sqrt{2}, 1, 1)$.

We give a different construction that allows to certify $\log_2 d$ bits of randomness in dimension $d=5$ here, and pursue the general question of rigid contextuality tests[15,46] certifying $\log_2 d$ bits for arbitrary d (as well as their monogamy relations[47,48] and the security proofs of the corresponding protocols) for future work.

Consider the orthogonality graph shown in Fig. 2. Without loss of generality, we consider $\langle u_1| = (1,0,0)$, $\langle u_{13}| = \frac{1}{\sqrt{1+x^2}}(x,1,0)$. Parametrizing $\langle u_2| = (0, \cos\theta_1, \sin\theta_1)$, $\langle u_3| = (0, \cos\theta_2, \sin\theta_2)$ and $\langle u_4| = (0, \cos\theta_4, \sin\theta_4)$ to ensure orthogonality with $\langle u_1|$, we deduce the following (unnormalized) vectors by taking appropriate cross products $\langle u_{11}| = (-\sin\theta_1, x\sin\theta_1, -x\cos\theta_1)$, $\langle u_5| = (-x, -\sin^2\theta_1, (1/2)\sin 2\theta_1)$, $\langle u_6| = (-\cos(\theta_1-\theta_2)\sin\theta_1, x\sin\theta_2, -x\cos\theta_2)$, $\langle u_7| = (-x, -\cos(\theta_1-\theta_2)\sin\theta_1\sin\theta_2, \cos(\theta_1-\theta_2)\sin\theta_1\cos\theta_2)$, $\langle u_{13}| = (-\sin\theta_3, x\sin\theta_3, -x\cos\theta_3)$, $\langle u_{10}| = (-x, -\sin^2\theta_3, (1/2)\sin 2\theta_3)$, $\langle u_9| = (\cos(\theta_2-\theta_3)\sin\theta_3, -x\sin\theta_2, x\cos\theta_2)$ and $\langle u_8| = (x, \cos(\theta_2-\theta_3)\sin\theta_2\sin\theta_3, -\cos(\theta_2-\theta_3)\cos\theta_2\sin\theta_3)$. We now ask what is the maximum value of the overlap $|\langle u_1|u_{13}\rangle| = \frac{x}{\sqrt{1+x^2}}$ under the constraint that $-\langle u_7|u_8\rangle = x^2 + \cos(\theta_1-\theta_2)\cos(\theta_3-\theta_2)\sin\theta_1\sin\theta_3$ equals 0. Or equivalently we wish to minimize $\cos(\theta_1-\theta_2)\cos(\theta_2-\theta_3)\sin\theta_1\sin\theta_3$. Setting the partial derivatives of this expression with respect to $\theta_1, \theta_2, \theta_3$ to equal zero, and finding the maximum overlap over all the solutions gives that $\theta_1 = -\theta_3 = \pi/4$ and $\theta_2 = 0$ with the optimal overlap $|\langle u_1|u_{13}\rangle| = 1/\sqrt{5}$. The addition of two other vertices u_{14}, u_{15} that are adjacent to all the vertices of the graph as well as to each other, gives the natural orthogonal

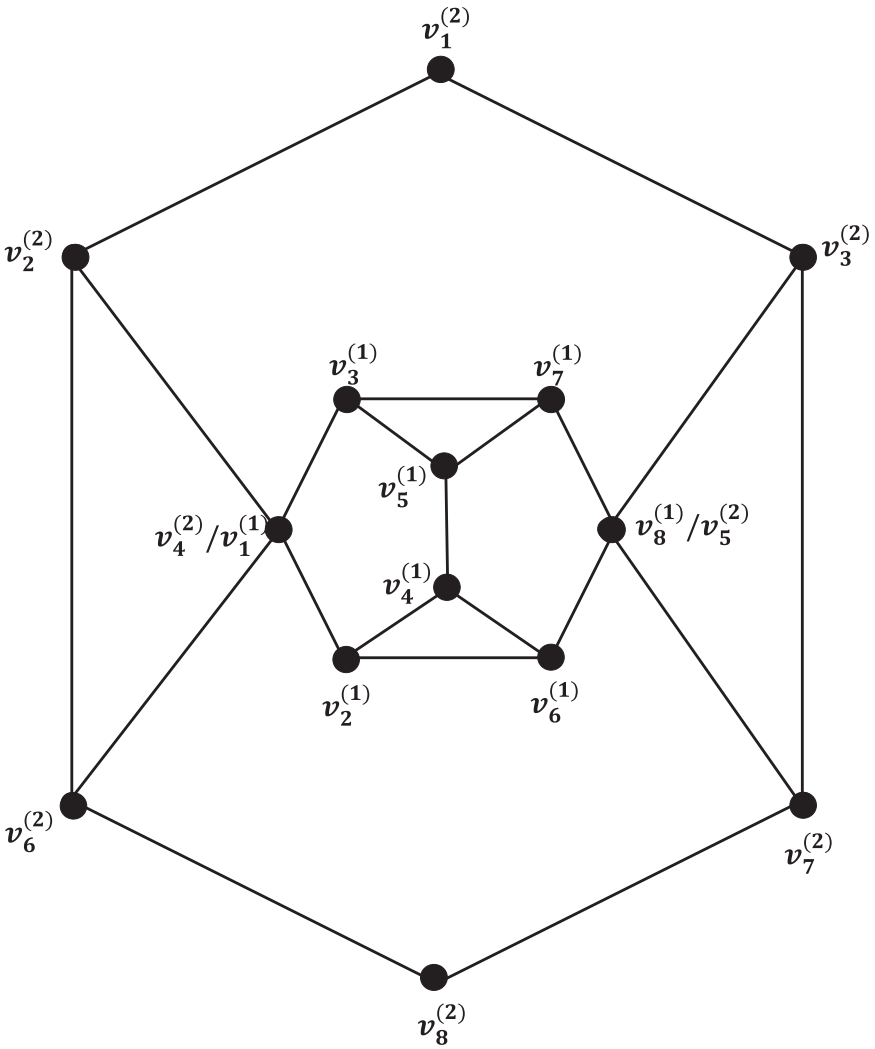

Fig. 1 An example illustrating the construction of a gadget with prescribed maximum overlap between the distinguished vectors $|v_1^{(2)}\rangle, |v_8^{(2)}\rangle$ of $\frac{1}{2}$ for any real orthogonal representation. The example illustrates the utility of gadgets in deriving contextuality tests that allow for optimal randomness certification for $d = 4$.

representation in dimension 5 with $\langle u_{14}| = (0, 0, 0, 1, 0)$ and $\langle u_{15}| = (0, 0, 0, 0, 1)$. We have thus constructed an extended 01-gadget in dimension 5 with the maximum overlap between the distinguished vertices being $\frac{1}{\sqrt{5}}$ (for any orthogonal representation in $\mathbb{R}^5$). While not a full self-testing statement, this indicates that the maximum violation of a non-contextuality inequality could allow to certify $\log_2 5$ bits for this construction. As stated earlier, we leave for future work the derivation of rigid contextuality tests based on gadgets to certify $\log_2 d$ bits for arbitrary dimension d and the security proofs of the corresponding (semi-device-independent) contextuality-based randomness generation.

Classical value of non-contextuality inequalities versus the weighted independence number

An interesting offshoot of the study of gadget structures is to point out a subtle modification in a famous result by Cabello, Severini and Winter (CSW) in[17,49] when the Kochen-Specker rules of exclusivity and completeness are enforced. In formulating the graph-theoretic approach to quantum correlations, CSW had considered general non-contextuality inequalities S as a positive linear combination of probabilities of events $S = \sum_i w_i P(e_i)$ with $w_i > 0$. For instance, the well-known KCBS inequality corresponding to the 5-cycle exclusivity graph is of the form $S_{KCBS} = \sum_{i=0}^{4} P(0, 1|i, i+1) \leq 2$ with 2 denoting the maximal value in all non-contextual hidden variable theories. In the CSW framework, one associates to every such non-contextuality inequality S a vertex-weighted graph (G, w) (note that a vertex-weighted graph (G, w) is a graph G with vertex set V and weight assignment $w : V \to \mathbb{R}_+$). The events e_i appearing in S are represented by vertices in G, adjacent vertices in G represent exclusive events (events e_i and e_j are exclusive if there exist jointly measurable observables μ_i and μ_j that distinguish between the events), and the vertex weights represent the coefficients w_i of the probabilities $P(e_i)$. The graph (G, w) is then called the exclusivity graph of S. The main result of CSW is the following theorem showing how the exclusivity graph of S can be used to calculate the optimal value of the inequality in classical and quantum theories.

Theorem 4. (Result 1 of CSW[17]). Given S corresponding to a non-contextuality inequality, the maximum value of S in classical and quantum theories is given by

$$S \overset{\text{NCHV}}{\leq} \alpha(G, w) \overset{\text{Q}}{\leq} \theta(G, w), \tag{8}$$

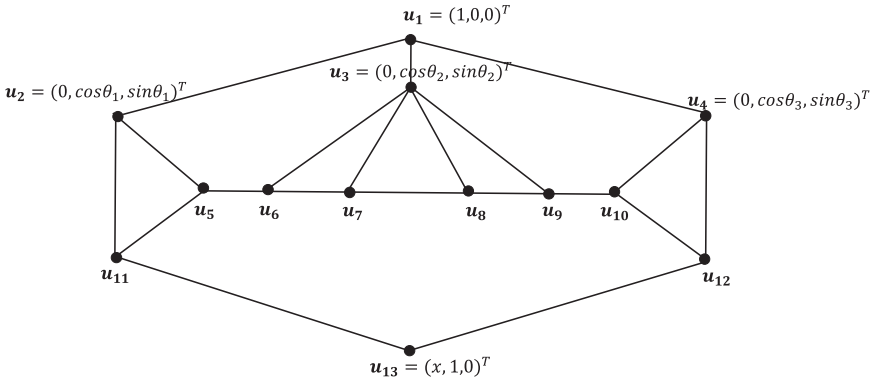

Fig. 2 An example illustrating the construction of a gadget with prescribed maximum overlap between the distinguished vectors $|u_1\rangle, |u_{13}\rangle$ of $\frac{1}{\sqrt{5}}$ for any real orthogonal representation. The example illustrates the utility of gadgets in deriving contextuality tests that allow for optimal randomness certification for $d = 5$.

where $\alpha(G, w)$ is the independence number of (G, w) and $\theta(G, w)$ is the Lovász-theta number of (G, w).

While it was recognized that $\theta(G, w)$ may only provide an upper bound to the quantum value in some cases - specifically when further constraints are imposed coming from the physical settings of the experiment, the statement that the classical value of any given non-contextuality inequality is given by $\alpha(G, w)$ is ubiquitous and taken to be true without any qualifications in much of the literature to this point. Furthermore, it is often also applied in situations when the Kochen-Specker rule of Completeness is enforced, namely that every maximum clique has exactly one vector that is assigned value 1. We now make the observation that this statement needs to be carefully considered in computing the classical value of non-contextuality inequalities arising from gadget-type structures, $\alpha(G, w)$ only provides an upper bound to the classical value for such inequalities when Completeness is enforced. Specifically consider a non-contextuality inequality S arising from a gadget-type exclusivity graph, so that vertex-weighted graph (G, w) corresponding to S is a gadget-type graph, meaning that the vertex set V of G can be partitioned into an independent set of distinguished vertices $V_{\text{dist}} \subset V$ and the non-distinguished vertices $V \setminus V_{\text{dist}}$. And furthermore, the weights w_i in S are given as

$$w_i = \begin{cases} 1 & i \in V_{\text{dist}} \\ 0 & i \in V \setminus V_{\text{dist}} \end{cases} \tag{9}$$

Observation 1
Given S corresponding to a non-contextuality inequality, the maximum value of S under the KS rules of Exclusivity and Completeness, in any classical (non-contextual hidden variable) theory is given by $\alpha(G, w)$ if and only if the vertex-weighted graph (G, w) is not of gadget-type.

Proof. The proof of the observation is a direct consequence of the gadget property of the exclusivity graph (G, w). By this gadget property, it holds that the vertices in the distinguished set V_{dist} cannot all be assigned value 1 in any non-contextual assignment when Completeness is enforced, despite the fact that V_{dist} is an independent set. Therefore, for the non-contextuality inequality $S = \sum_i w_i P(e_i)$ with w_i given by Eq. (9), the maximum value in any non-contextual hidden variable theory is only upper bounded by and never equal to $\alpha(G, w)$ (note that achieving $\alpha(G, w)$ requires assigning value 1 to every vertex in the independent set V_{dist}). Furthermore, this restriction on the assignment of 1s (arising from the KS requirement that every measurement returns an outcome) is exactly the defining feature of gadget-type graphs so that $\alpha(G, w)$ is not equal to the classical value (under Completeness) only for the non-contextuality inequalities arising from such measurement structures.

A generalization of gadgets with other forbidden value assignments

Thus far, we have generalized the well-known 'True-implies-False' sets or 01-gadgets to gadgets of order (m, k). These latter sets contain m independent vertices (mutually non-orthogonal vectors) of which exactly k may be assigned value 1 in any $\{0, 1\}$-coloring. In other words, given an independent set $I = \{v_1, \ldots, v_m\}$ these consider forbidden value assignments of the form $\{\underbrace{1, \ldots, 1}_{k+1}, f(v_{k+2}), \ldots, f(v_m)\}$ and permutations thereof, where $f: V \to \{0, 1\}$ is any $\{0, 1\}$-coloring of the vertices. One may consider a yet more general measurement structure in which we specify a set of forbidden value assignments $\mathcal{H} \subset \{0, 1\}^m$. The usual 'True-implies-False' sets then correspond to $\mathcal{H} = \{(1, 1)\}$ for a given independent set $I = \{v_1, v_2\}$ of two vertices.

Definition 10. A $\{0, 1\}$-colorable set $S_{gad} \in \mathbb{C}^d$ is a gadget in dimension d for a specified forbidden set $\mathcal{H} \subset \{0, 1\}^m$ if it contains an (ordered) set of mutually non-orthogonal vectors $I = \{|v_1\rangle, \ldots, |v_m\rangle\}$ such that in any $\{0, 1\}$-coloring of S_{gad} it holds that $f(I) \in \{0, 1\}^m \setminus \mathcal{H}$.

Equivalently, the generalized gadget for a forbidden assignment $\mathcal{H}$ can be defined in graph-theoretic terms as follows.

Definition 11. A $\{0, 1\}$-colorable graph $G = (V, E)$ is a gadget in dimension d for a specified forbidden set $\mathcal{H} \subset \{0, 1\}^m$, if it has faithful dimension $d^*(G_{gad}) = \omega(G_{gad}) = d$ and contains an (ordered) independent set $I \subset V$ of cardinality $|I| = m$ such that in any $\{0, 1\}$-coloring $f: V \to \{0, 1\}$ it holds that $f(I) \in \{0, 1\}^m \setminus \mathcal{H}$.

A natural question then arises - can a gadget be constructed for every forbidden set $\mathcal{H} \subset \{0, 1\}^m$ for arbitrary $m \geq 2$? Note that the number of such forbidden sets $\mathcal{H}$ is $2^{2^m} - 1$ (i.e., all subsets of $\{0, 1\}^m$ except the empty set). We answer this question in the affirmative and demonstrate the precise steps of building such a gadget in Supplementary Information Note 4. It's worth noting that Kochen Specker proofs themselves come under the umbrella of the generalized gadget structures defined here, with $\mathcal{H} = \{0, 1\}^m$ for some independent set in the graph I of size $|I| = m$ and for arbitrary $m \geq 1$. In other words, there is no valid $\{0, 1\}$-assignment to the vertices of the independent set I.

DATA AVAILABILITY

The authors declare that the data supporting the findings of this study are available within the paper and in the Supplementary Information.

Received: 31 August 2022; Accepted: 8 June 2023;
Published online: 29 June 2023

REFERENCES

1. Kochen, S. & Specker, E. P. The problem of hidden variables in quantum mechanics. *J. Math. Mech.* **17**, 59–87 (1967).
2. Bell, J. B. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.* **38**, 447 (1966).
3. Clifton, R. Getting contextual and nonlocal elements-of-reality the easy way. *Am. J. Phys.* **61**, 443–447 (1993).
4. Stairs, A. Quantum logic, realism, and value definiteness. *Philos. Sci.* **50**, 578–602 (1983).
5. Hardy, L. Nonlocality for two particles without inequalities for almost all entangled states. *Phys. Rev. Lett.* **71**, 1665 (1993).
6. Belinfante, F. J. *A Survey of Hidden-Variables Theories* (Pergamon Press, 1973).
7. Ramanathan, R. et al. Gadget structures in proofs of the Kochen-Specker theorem. *Quantum* **4**, 308 (2020).
8. Cabello, A. & García-Alcaine, G. Bell-Kochen-Specker theorem for any finite dimension. *J. Phys. A: Math. Gen.* **29**, 1025 (1996).
9. Cabello, A., Portillo, J. R., Solís, A. & Svozil, K. Minimal true-implies-false and true-implies-true sets of propositions in noncontextual hidden-variable theories. *Phys. Rev. A* **98**, 012106 (2018).
10. Cubitt, T. S., Leung, D., Matthews, W. & Winter, A. Improving zero-error classical communication with entanglement. *Phys. Rev. Lett.* **104**, 230503 (2010).
11. Um, M. et al. Experimental certification of random numbers via quantum contextuality. *Sci Rep.* **3**, 1627 (2013).
12. Horodecki, K. et al. Contextuality offers device-independent security. Preprint at https://arxiv.org/abs/1006.0468 (2010).
13. Howard, M., Wallman, J., Veitch, V. & Emerson, J. Contextuality supplies the 'magic' for quantum computation. *Nature* **510**, 351–355 (2014).
14. Gupta, S., Saha, D., Xu, Z.-P., Cabello, A. & Majumdar, A. S. Quantum contextuality provides communication complexity advantage. *Phys. Rev. Lett.* **130**, 080802 (2023).
15. Bharti, K. et al. Robust self-testing of quantum systems via noncontextuality inequalities. *Phys. Rev. Lett.* **122**, 250403 (2019).
16. Kleinmann, M. & Cabello, A. Quantum correlations are stronger than all non-signaling correlations produced by n-outcome measurements. *Phys. Rev. Lett.* **117**, 150401 (2016).
17. Cabello, A., Severini, S. & Winter, A. Graph-theoretic approach to quantum correlations. *Phys. Rev. Lett.* **112**, 040401 (2014).
18. Kleinmann, M., Vértesi, T. & Cabello, A. Proposed experiment to test fundamentally binary theories. *Phys. Rev. A* **96**, 032104 (2017).
19. Cabello, A., Estebaranz, J. M. & García-Alcaine, G. Bell-Kochen-Specker theorem: A proof with 18 vectors. *Phys. Lett. A* **212**, 183–187 (1996).
20. Cabello, A. Experimentally testable state-independent quantum contextuality. *Phys. Rev. Lett.* **101**, 210401 (2008).
21. Lovász, L., Saks, M. & Schrijver, A. Orthogonal representations and connectivity of graphs. *Linear Alg. Appl.* **114**, 439–454 (1989).
22. Aksionov, V. A. & Mel'nikov, L. S. Essay on the theme: The three-color problem. *Colloq. Math. Soc. Janos Bolyai.* **18**, 23–34 (1978).
23. Aksionov, V. A. & Mel'nikov, L. S. Some counterexamples associated with the three-color problem. *J. Comb. Theory. Ser. B.* **28**, 1–9 (1980).
24. Erdös, P. & Stone, A. H. On the structure of linear graphs. *Bull. Am. Math. Soc.* **52**, 1087–1091 (1946).
25. Kochen, S. & Specker, E. P. Logical structures arising in quantum theory. In *Ernst Specker Selecta* (ed. Hughes, R. I. G.) 209–221 (Springer, 1990).
26. Greechie, R. J. Some results from the combinatorial approach to quantum logic. In *Logic and Probability in Quantum Mechanics* (ed. Suppes, P.) 105–119 (Springer, 1976).
27. Pitowsky, I. Betting on the outcomes of measurements: a Bayesian theory of quantum probability. *Stud. Hist. Philos. Sci. B: Stud. Hist. Philos. Mod. Phys.* **34**, 395–414 (2003).
28. Pitowsky, I. Quantum mechanics as a theory of probability. In *Physical Theory and its Interpretation: Essays in Honor of Jeffrey Bub* (eds. Hemmo, M. & Shenker, O.) 213–240 (Springer, 2006).
29. Arends, F. *A Lower Bound on the Size of the Smallest Kochen-specker Vector System in Three Dimensions* (University of Oxford, 2009).
30. Mermin, N. D. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.* **65**, 3373 (1990).
31. Yu, S. & Oh, C. H. State-independent proof of Kochen-Specker theorem with 13 rays. *Phys. Rev. Lett.* **108**, 030402 (2012).
32. Navascués, M., Guryanova, Y., Hoban, M. J. & Acín, A. Almost quantum correlations. *Nat. Commun.* **6**, 6288 (2015).
33. Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.* **10**, 073013 (2008).
34. Nemhauser, G. & Trotter, L. Vertex packing: structural properties and algorithms. *Math. Program.* **8**, 232–248 (1975).
35. Balinski, M. L. Integer programming: methods, uses, computations. *Manage. Sci.* **12**, 253–313 (1965).
36. Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
37. Colbeck, R. & Renner, R. Free randomness can be amplified. *Nat. Phys.* **8**, 450–453 (2012).
38. Kessler, M. & Arnon-Friedman, R. Device-independent randomness amplification and privatization. *IEEE JSAIT* **1**, 568–584 (2020).
39. Ramanathan, R. et al. Randomness amplification against no-signaling adversaries using two devices. *Phys. Rev. Lett.* **117**, 230501 (2016).
40. Grudka, A. et al. Free randomness amplification using bipartite chain correlations. *Phys. Rev. A* **90**, 032322 (2014).
41. Brandão, F. G. S. L. et al. Realistic noise-tolerant randomness amplification using finite number of devices. *Nat. Commun.* **7**, 1–6 (2016).
42. Abbott, A. A., Calude, C. S. & Svozil, K. A variant of the Kochen-Specker theorem localising value indefiniteness. *J. Math. Phys.* **56**, 102201 (2015).
43. Abbott, A. A., Calude, C. S. & Svozil, K. A quantum random number generator certified by value indefiniteness. *Math. Struct. Comput. Sci.* **24**, e240303 (2014).
44. Klyachko, A. A., Can, M. A., Binicioğlu, S. & Shumovsky, A. S. Simple test for hidden variables in spin-1 systems. *Phys. Rev. Lett.* **101**, 020403 (2008).
45. Hrushovski, E. & Pitowsky, I. Generalizations of Kochen and Specker's theorem and the effectiveness of Gleason's theorem. *Stud. Hist. Philos. Sci. B: Stud. Hist. Philos. Mod. Phys.* **35**, 177–194 (2004).
46. Ramanathan, R., Liu, Y. & Horodecki, P. Large violations in Kochen Specker contextuality and their applications. *New J. Phys.* **24**, 033035 (2022).
47. Ramanathan, R., Soeda, A., Kurzyński, P. & Kaszlikowski, D. Generalized monogamy of contextual inequalities from the no-disturbance principle. *Phys. Rev. Lett.* **109**, 050404 (2012).
48. Saha, D. & Ramanathan, R. Activation of monogamy in non-locality using local contextuality. *Phys. Rev. A* **95**, 030104 (2017).
49. Cabello, A., Severini, S. & Winter, A. (Non-) Contextuality of physical theories as an axiom. Preprint at https://arxiv.org/abs/1010.2163 (2010).

ACKNOWLEDGEMENTS

L.Y. and R.R. acknowledge support from the Start-up Fund "Device-Independent Quantum Communication Networks" from The University of Hong Kong, the Early Career Scheme (ECS) grant "Device-Independent Random Number Generation and Quantum Key Distribution with Weak Random Seeds" (Grant No. 27210620), the General Research Fund (GRF) grant "Semi-device-independent cryptographic applications of a single trusted quantum system" (Grant No. 17211122) and the Research Impact Fund (RIF) "Trustworthy quantum gadgets for secure online communication" (Grant No. R7035-21). K.H., M.R., and P.H. acknowledge partial support by the Foundation for Polish Science (IRAP project, ICTQT, contract no. MAB/2018/5, co-financed by EU within Smart Growth Operational Programme). The 'International Centre for Theory of Quantum Technologies' project (contract no. MAB/2018/5) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3).

AUTHOR CONTRIBUTIONS

The project was conceived by R.R., L.Y., and K.H., and all authors discussed extensively and contributed to the development of the theory and content presented in the manuscript. The initial draft of the manuscript was written by R.R., L.Y., and K.H., and it was critically reviewed and revised by P.H. before the final approval of the completed version by all authors.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-023-00728-2.

Correspondence and requests for materials should be addressed to Ravishankar Ramanathan.

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

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