Contextual hypergraphs

Petr Lisonek
Simon Fraser University
Burnaby, BC, Canada

Some parts are joint work with Stefan Trandafir (SFU).

Carleton Finite Fields eSeminar
24 June 2020

Hypergraphs/incidence structures and configurations

A *hypergraph (incidence structure)* (V, E) consists of a finite set V of *vertices (points)* and a set E of *edges (blocks)*, each of which is a non-empty subset of V.

A *configuration* (v_k, b_ℓ) is a hypergraph with v vertices, each of which belongs to k blocks, and with b blocks, each of size ℓ.

A *configuration* (v_k, v_k) is abbreviated as (v_k). It is called *self-dual* if it is isomorphic to its dual (exchange roles of points and blocks, preserve the incidence relation).

Point labellings

We'll be labelling points of the hypergraph as follows. Fix a positive integer n. Each point will be labelled by a matrix $A \in \mathbb{C}^{n \times n}$ such that:

- $A^2 = I$
- $A^* = A$ (A is Hermitian)
- $AB = BA$ if A, B occur as labels in the same block
- The product of labels in each block is either I or $-I$.

Let us say that a point labelling is *admissible* if it satisfies all these conditions, for each point and each block.

Contextual hypergraph

Definition

A hypergraph is called *contextual* if

1. Each point belongs to an *even* number of blocks.
2. There exists an admissible labelling of points such that the number of blocks whose label product is $-I$ is *odd*. (We'll call such point labelling *contextual*.)

The above definition is one special way of formalizing *contextuality* mathematically. There exist *many other* formalizations of contextuality.

Our goal is to use finite fields and other combinatorial ingredients to construct contextual hypergraphs.

Hidden variable theories

In 1935, Einstein, Podolsky and Rosen hinted at the possibility of classical descriptions of quantum mechanics in which the randomness of quantum measurement was modelled by a hidden probabilistic parameter. These models have become known as *hidden variable theories;* they postulate that measurement outcomes are pre-existing and that they are merely revealed by measurements.

Einstein: "God does not play dice with the universe."

Contextuality

On the other hand, *contextuality* is a property of quantum mechanics which means that measurement outcomes depend on the contexts in which the measurements are performed. These contexts are the edges of our hypergraphs, and measurements are described by the labels on these edges. Assuming our previous definition, a contextual hypergraph is a demonstration (also called "parity proof") of contextuality.

Contextuality can be also noticed in psychology and in other areas.

A quantum computation resource

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

There exist models of quantum computation specifically utilizing contextuality.

Pauli operators

Let

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

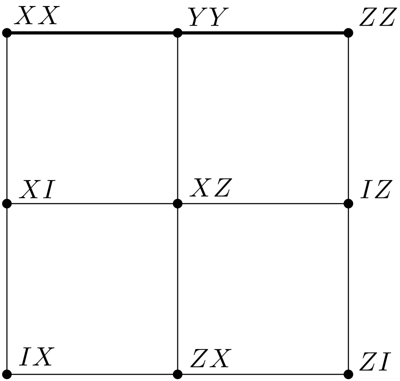
be the well known *Pauli matrices*, where $i^2 = -1$.

Proposition

We have

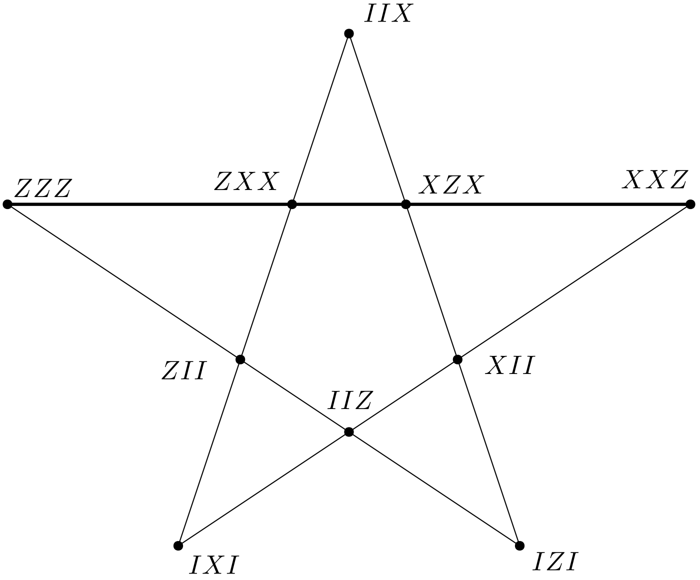
1. I, X, Y, Z *are Hermitian,*
2. X, Y, Z *pairwise anti-commute:* $XY = -YX$, $YZ = -ZY$, $XZ = -ZX$,
3. $X^2 = Y^2 = Z^2 = I$,
4. $XYZ = iI$.

A contextual $(9_2, 6_3)$ configuration (Mermin 1993)



For $P_i \in \{I, X, Y, Z\}$ the notation $P_1 P_2 \cdots P_k$ is a shorthand for $P_1 \otimes P_2 \otimes \cdots \otimes P_k$, an operator in $\mathbb{C}^{2^k \times 2^k}$.

A contextual $(10_2, 5_4)$ configuration (Mermin 1993)



2-regular contextual hypergraphs

Theorem (Arkhipov 2013)

Let H be a proper 2-regular hypergraph. Let G be the dual graph of H. Then H is contextual if and only if G is non-planar.

Proof uses Kuratowski's Theorem (graph is planar iff it does not contain K_5 or $K_{3,3}$ as a minor). Note that the two configurations on the previous two slides are the duals of $K_{3,3}$ and K_5, respectively.

Pauli operators as symplectic vectors

Via the correspondence $I \leftrightarrow 00$, $X \leftrightarrow 10$, $Z \leftrightarrow 01$, $Y \leftrightarrow 11$, a k-fold tensor product $P_1 P_2 \cdots P_k = P_1 \otimes P_2 \otimes \cdots \otimes P_k$ can be represented as a $2k$-dimensional binary vector.

Vice versa, let $\mathcal{P}(v)$ denote the Pauli operator represented by $v \in \mathbb{F}_2^{2k}$. Let

$$x \odot y = \sum_{i=1}^{k} x_{2i-1} y_{2i} + y_{2i-1} x_{2i}$$

be a *symplectic inner product* on $\mathbb{F}_2^{2k}$. We have for all $x, y \in \mathbb{F}_2^{2k}$

$$\mathcal{P}(x)\mathcal{P}(y) = (-1)^{x \odot y} \mathcal{P}(y)\mathcal{P}(x).$$

Families of contextual hypergraphs

Historically, contextual hypergraphs (or other contextual structures) have been found mostly by computer search.

While we also use computational methods to some extent, we ultimately aim at computer-free, systematical constructions. Specifically we focus on three families of contextual hypergraphs:

1. Hypergraphs of Kochen-Specker type
2. Coxeter configurations
3. Configurations arising from group developments

Construction 1: Using Kochen-Specker pairs

Kochen and Specker (1965) exhibited the first contextual structure, consisting of 117 vectors in $\mathbb{R}^3$. Motivated by their work, the following structures have been studied:

Definition

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 for $i = 1, \ldots, k$ 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.

Kochen-Specker pairs and contextual hypergraphs

Any KS pair as defined on the previous page produces a contextual hypergraph, as follows:

For any vector $v \in \mathcal{V}$ let R_v be the operator that represents the reflection of $\mathbb{C}^n$ about the hyperplane $v^\perp$. Let $\mathcal{V}$ be the vertex set of the hypergraph and let edges of the hypergraph be the bases B_i. Let R_v be the label of v. We can easily check that this is an admissible vertex labelling, and in particular $\prod_{v \in B_i} R_v = -I$ for each i. Since the number of edges is odd, we have produced a contextual hypergraph.

Notation

We work with the usual inner product on $\mathbb{C}^n$ defined by $\langle x, y\rangle = \sum_{i=1}^{n} x_i \overline{y_i}$. 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.

For $x, y \in \mathbb{C}^n$ we define

$$x \circ y = (x_1 y_1, \ldots, x_n y_n).$$

Note that for $x, y, z \in \mathbb{C}^n$ such that z is unimodular we have

$$\langle z \circ x, z \circ y\rangle = \langle x \circ z, y \circ z\rangle = \sum_{i=1}^{n} x_i z_i \overline{y_i z_i} = \langle x, y\rangle.$$

Generalized Hadamard matrices

Definition

Let G be a group of order g and let λ be a positive integer. A *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 λ times among the differences $m_{k,j} - m_{\ell,j}$, $1 \leq j \leq g\lambda$. Such matrix is denoted $\mathrm{GH}(g, \lambda)$.

Many infinite families of $\mathrm{GH}(g, \lambda)$ are known (direct constructions and recursive constructions). Several constructions of GH matrices use finite fields.

Letting $\zeta_g = e^{2\pi\sqrt{-1}/g}$ and $H = (h_{i,j})$ where $h_{i,j} = \zeta_g^{m_{i,j}}$ we get a complex Hadamard matrix H of order $g\lambda$.

Infinite families of KS pairs

Theorem (L. 2017)

Assume that $g > 2$ *and* $\lambda > 0$ *are such that* $\mathrm{GH}(g, \lambda)$ *over* $\mathbb{Z}_g$ *exists and* $n = g\lambda$ *is even. Then there exists a Kochen-Specker pair* $(\mathcal{V}, \mathcal{B})$ *in* $\mathbb{C}^n$ *with* $|\mathcal{V}| \leq \binom{n+1}{2}$ *and* $|\mathcal{B}| = n + 1$.

Applying this theorem with $g = 3$ and $\lambda = 2$ (hence $n = 6$) we get the "simplest" KS set. (L. 2013)

Proof.

Let M be the $\mathrm{GH}(g,\lambda)$ over $\mathbb{Z}_g$ whose existence is assumed, and let $H = (h_{i,j}) = \zeta_g^{m_{i,j}}$ be the corresponding complex Hadamard matrix. Let h_i denote the i-th row of H. W.l.o.g. we assume $h_1 = (1, 1, \ldots, 1)$, equivalently $m_1 = (0, 0, \ldots, 0)$.

Let the elements of $\mathcal{V}$ be denoted $v^{\{r,s\}}$ where $1 \leq r, s \leq n+1$, $r \neq s$. Note $v^{\{r,s\}} = v^{\{s,r\}}$ for all $r \neq s$.

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 $v^{\{r,s\}} = h_{r-1} \circ h_{s-1}$.

Infinite families of KS pairs (cont'd)

For $1 \leq r \leq n+1$ let

$$B_r = \{v^{\{r,i\}} \,:\, 1 \leq i \leq n+1,\ i \neq r\}$$

and let $\mathcal{B} = (B_1, \ldots, B_{n+1})$. We will now prove that each B_r is an orthogonal basis of $\mathbb{C}^n$. There are several cases to distinguish.

For $2 < r, s, t \leq n+1$ and r, s, t distinct we have

$$\langle v^{\{r,s\}}, v^{\{r,t\}} \rangle = \langle h_{r-1} \circ h_{s-1}, h_{r-1} \circ h_{t-1} \rangle = \langle h_{s-1}, h_{t-1} \rangle = 0.$$

Infinite families of KS pairs (cont'd)

Let $r = 1$. For $1 < s < t \leq n+1$ we have

$$\langle v^{\{1,s\}}, v^{\{1,t\}} \rangle = \langle h_{s-1}, h_{t-1} \rangle = 0.$$

Let $r = 2$. Recall that $g > 2$. For distinct $s, t > 2$ we have

$$\begin{aligned}\langle v^{\{2,s\}}, v^{\{2,t\}} \rangle &= \langle h_{s-1} \circ h_{s-1}, h_{t-1} \circ h_{t-1} \rangle \\ &= \sum_{i=1}^{g\lambda} \zeta_g^{2(m_{s-1,i} - m_{t-1,i})} = \lambda \sum_{i=0}^{g-1} \zeta_g^{2i} = \lambda \frac{\zeta_g^{2g} - 1}{\zeta_g^2 - 1} = 0.\end{aligned}$$

Also for $t > 2$ we have

$$\begin{aligned}\langle v^{\{2,t\}}, v^{\{2,1\}} \rangle &= \langle h_{t-1} \circ h_{t-1}, \mathbf{1} \rangle \\ &= \sum_{i=1}^{g\lambda} \zeta_g^{2m_{t-1,i}} = 0.\end{aligned}$$

Infinite families of KS pairs (cont'd)

Now let $2 < r \leq n+1$. For $t > 2$, $t \neq r$ we have

$$\begin{aligned}\langle v^{\{r,1\}}, v^{\{r,t\}} \rangle &= \langle h_{r-1}, h_{r-1} \circ h_{t-1} \rangle = \langle h_{r-1} \circ h_1, h_{r-1} \circ h_{t-1} \rangle = \\ &= \langle h_1, h_{t-1} \rangle = 0\end{aligned}$$

as well as

$$\begin{aligned}\langle v^{\{r,2\}}, v^{\{r,t\}} \rangle &= \langle h_{r-1} \circ h_{r-1}, h_{r-1} \circ h_{t-1} \rangle \\ &= \langle h_{r-1}, h_{t-1} \rangle = 0.\end{aligned}$$

Finally we have

$$\begin{aligned}\langle v^{\{r,1\}}, v^{\{r,2\}} \rangle &= \langle h_{r-1}, h_{r-1} \circ h_{r-1} \rangle \\ &= \langle h_1 \circ h_{r-1}, h_{r-1} \circ h_{r-1} \rangle = \langle h_1, h_{r-1} \rangle = 0.\end{aligned}$$

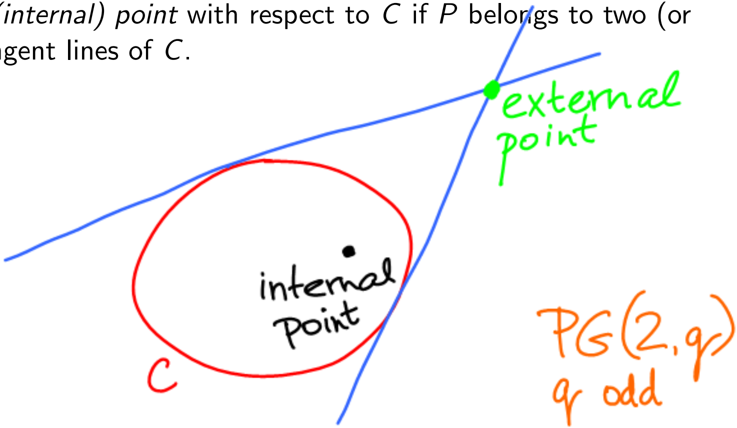
Infinite families of KS pairs (cont'd)

We note that $|\mathcal{B}| = n+1$ is odd since n is assumed to be even. We will complete the proof by verifying that each element of $\mathcal{V}$ belongs to an even number of bases B_r. 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 $(v^{\{i,j\}})_{1 \le i < j \le n+1}$ 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 $j \neq k$ implies $v^{\{i,j\}} \neq v^{\{i,k\}}$ as $\langle v^{\{i,j\}}, v^{\{i,k\}} \rangle = 0$.

Construction 2: Coxeter configurations

Let q be an odd prime power. Let C be a non-degenerate quadric (conic) in $\mathrm{PG}(2, q)$, the classical projective plane over $\mathbb{F}_q$.

If P is a point in this plane and P is not on C, then P is called an *external (internal) point* with respect to C if P belongs to two (or none) tangent lines of C.



Coxeter configurations

Coxeter (Proc. London Math. Soc. 1983) considers the following configuration: The points are the $\binom{q}{2}$ internal points of C, and the blocks are the $\binom{q}{2}$ non-secants of C (lines disjoint from C). This is a self-dual configuration of type $\left(\binom{q}{2}_{\frac{q+1}{2}}\right)$. Let $C(q)$ denote this configuration.

Could $C(q)$ be contextual? For which q?

Let us restrict attention to labellings by Pauli operators, which we'll represent by symplectic vectors as introduced above. Recall that Pauli operators $\mathcal{P}(x)$ and $\mathcal{P}(y)$ commute iff $x \odot y = 0$.

Gram matrices in symplectic spaces

Theorem (Godsil & Royle)

Let M be a square matrix over $\mathbb{F}_2$ with zero diagonal, no zero row, and no repeated rows. Then M is a Gram matrix of a set of vectors in $2k$-dimensional symplectic space over $\mathbb{F}_2$ if and only if the rank of M is at most $2k$.

It is simpler to work with the Gram matrix instead of trying to find an explicit contextual labelling!

Gram matrices for contextual hypergraphs

As is common, call points x, y *collinear* if they occur together in some block. Let $L(x)$ be the label of vertex x in some contextual labelling L. We know that $L(x) \odot L(y) = 0$ if x, y are collinear.

However, if x, y are not collinear, both $L(x) \odot L(y) = 0$ and $L(x) \odot L(y) = 1$ are possible. Which one should we choose?

Denote M_x the row of M corresponding to vertex x. W.l.o.g. assume that the labelling is done in the smallest possible dimension, then it is not difficult to see that $\sum_{x \in e} M_x = \mathbf{0}$ for each hyperedge e. Altogether, the set of matrices that can occur as Gram matrices for a given hypergraph is a vector space over $\mathbb{F}_2$.

Coming back to the configurations $C(q)$, they are not contextual for $q < 7$. For $C(7)$ only one non-trivial Gram matrix is possible, in which $L(x) \odot L(y) = 1$ for any pair of non-collinear points x, y; the rank of this matrix is 8.

Gram matrices for contextual hypergraphs

Can we determine just from the Gram matrix whether the labelling is contextual? The last remaining issue is to find whether the number of blocks with label products $-I$ is odd. Equivalently we ask if P, the product of all block products, equals $-I$.

Gram matrices for contextual hypergraphs

Proposition (L., Trandafir 2020)

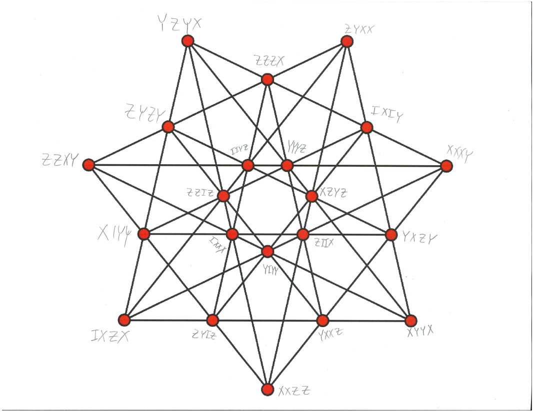
Fix an arbitrary ordering of all hyperedges and list them in the form $(v_1, \ldots, v_n)$ where each v_i is a vertex; the ordering of vertices inside each hyperedge is also arbitrary. Impose a total order $\prec$ on the set of vertices. Then M is a Gram matrix of a contextual labelling with Pauli operators if and only if

$$\sum_{i<j,\ v_i \succ v_j} M_{i,j} = 1.$$

Proof sketch: We have $P = L(v_1) \cdots L(v_n)$. By swapping pairs of adjacent factors in this product and keeping track whether they commuted or not, we bring P in the form where each factor is $L(x)^2 = I$ for some vertex x, and the formula displayed above determines the $\pm$ sign in front of this product.

Contextual (21_4) configuration

This is $C(7)$ in the previous notation. The contextuality can be determined already by the previous proposition. The contextual labelling was obtained using subgraph embedding function in Sage. This configuration was likely studied before Coxeter's paper (Felix Klein and others). The product of labels is $-I$ along each block.



Contextual Coxeter configurations

Conjecture

If $q \equiv 7, 11 \pmod{16}$ then $C(q)$ admits a contextual labelling with Pauli operators.

We verified this computationally for $q \leq 59$, using the Gram matrix M that assigns $M_{x,y} = 1$ to any non-collinear pair x, y.

This could be a nice problem in finite geometry.

Construction 3: Configurations arising from group developments

Let $(G, +)$ be an abelian group (this can be further relaxed). Let S be a non-empty subset of G, and denote $|G| = v$, $|S| = s$. We can construct a (v_s) configuration as follows. The points are the elements of G. The blocks are of the form $S + g$ where $g \in G$. This type of construction is well known in design theory. The set S is sometimes called the "starter."

G is a group of automorphisms of the constructed configuration; in particular the configuration is vertex-transitive. This is recognized as an added value in the quantum mechanics applications.

Configurations arising from group developments

We are currently working to classify abelian groups G that lead to contextual configurations. Some initial computations suggest that the elementary abelian groups $\mathbb{Z}_3^n$ are promising in particular. So far we have found contextual $((3^n)_k)$ configurations for $(n, k) = (3, 4), (4, 6), (5, 6), (6, 8)$, among others.

Hypergraphs that are not contextual

For some hypergraphs it is possible to prove that they are not contextual, as follows.

The conditions for an admissible vertex labelling can be all written in the form of a finitely presented group, and the vertex labels are elements of this group. Let the product of all products of labels along an edge be denoted P. We know that the labelling proves that the hypergraph is contextual iff $P = -I$.

Hypergraphs that are not contextual

The *Knuth-Bendix algorithm* attempts to form a confluent rewriting system that simplifies any element of the group to its unique canonical form. (Two elements of the group are equal if they reduce to the same canonical form.) Since the word problem for finitely presented groups is in general undecidable, the Knuth-Bendix algorithm can not always succeed. If it does succeed for the group corresponding to the given hypergraph, and if subsequently P reduces to the canonical form I, then we know that the hypergraph is not contextual.

In this way we have proved:

Theorem (L. 2019)

For $v \leq 18$ no configuration (v_4) is contextual.

Summary

While contextuality is an intrinsic and important property of quantum mechanics, it is possible to formulate it purely mathematically, at various levels and in various ways.

Construction of configurations that exhibit contextuality is of interest, to enable lab experiments and possibly provide building blocks for quantum computing.

Discrete mathematics and specifically finite fields play an important role in these constructions.