From informationally complete POVMs to the Kochen-Specker theorem

Michel Planat

Université de Bourgogne/Franche-Comté, Institut FEMTO-ST CNRS UMR 6174, 15 B Avenue des Montboucons, F-25044 Besançon, France.
michel.planat@femto-st.fr

Quantum Contextuality in Quantum Mechanics and Beyond, Prague, Czech Republic, June 4-5 (2017).

- It is possible to conciliate informationally complete measurements on an unknown density matrix: IC-POVMs and Kochen-Specker (KS) concepts (which forbid hidden variable theories of a non-contextual type). This was shown for qutrits [1] and it is continued here for two-qubits (2QB), three-qubits (3QB) and two and three qutrits (2QT & 3QT). Non symmetric IC-POVMs have been found in dimensions 3 to 12 starting from **permutation groups**, the derivation of appropriate non-stabilizer states: **magic/fiducial states** and the action of the **Pauli group** on them [2]. For 2QB, 3QB, 2QT and 3QT systems,a Kochen-Specker theorem follows.

[1] I. Bengtsson, K. Blanchfield and A. Cabello, A Kochen-Specker inequality from a SIC, *Phys. Lett.* **A376** 374-376 (2012).

[2] M. Planat and Rukhsan-Ul-Haq, The magic of universal quantum computing with permutations, arxiv 1701.06443 (quant-ph).

A reminder on SIC-POVMs

- A POVM is a collection of positive semi-definite operators $\{E_1, \dots, E_m\}$ that sum to the identity. In the measurement of a state ρ, the i-th outcome is obtained with a probability given by the **Born rule** $p(i) = \mathrm{tr}(\rho E_i)$. For a **minimal IC-POVM**, one needs d^2 one-dimensional projectors $\Pi_i = |\psi_i\rangle\langle\psi_i|$, with $\Pi_i = dE_i$, such that the rank of the Gram matrix with elements $\mathrm{tr}(\Pi_i \Pi_j)$, is precisely d^2.
- A **SIC-POVM** further obeys the relation (Renes et al,2004)

$$|\langle\psi_i|\psi_j\rangle|^2 = \mathrm{tr}(\Pi_i \Pi_j) = \frac{d\delta_{ij} + 1}{d+1},$$

This allows the recovery of the density matrix as (Fuchs, 2004)

$$\rho = \sum_{i=1}^{d^2} \left[(d+1)p(i) - \frac{1}{d}\right] \Pi_i.$$

This type of quantum tomography is often known as quantum-Bayesian, where the $p(i)$'s represent agent's Bayesian degrees of belief.

- One starts from the qubit magic/fiducial state

$$|T\rangle = \cos(\beta)\,|0\rangle + \exp\left(\frac{i\pi}{4}\right)\sin(\beta)\,|1\rangle\,, \quad \cos(2\beta) = \frac{1}{\sqrt{3}},$$

employed for **universal quantum computation** (Bravyi, 2004). It is defined as the $\omega_3 = \exp(\frac{2i\pi}{3})$-eigenstate of the SH matrix [the product of the Hadamard matrix H and the phase gate $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$].

- Taking the **action on** $|T\rangle$ **of the four Pauli gates** I, X, Z and Y, the corresponding (pure) projectors $\Pi_i = |\psi_i\rangle\langle\psi_i|\,, i = 1\ldots4$, sum to twice the identity matrix thus building a POVM and the pairwise distinct products satisfy $|\langle\psi_i|\psi_j\rangle|^2 = \frac{1}{3}$. The four elements Π_i form the well known 2-**dimensional SIC-POVM**.

In contrast, there is no POVM attached to the magic state $|H\rangle = \cos(\frac{\pi}{8})\,|0\rangle + \sin(\frac{\pi}{8})\,|1\rangle$.

- Later, **we construct IC-POVMs using the covariance with respect to the generalized *d*-dimensional Pauli group** that is generated by the shift and clock operators as follows

$$X|j\rangle = |j+1 \mod d\rangle$$
$$Z|j\rangle = \omega^j |j\rangle \quad (1)$$

with $\omega = \exp(2i\pi/d)$ a d-th root of unity.

A general Pauli (also called Heisenberg-Weyl) operator is of the form

$$T_{(m,j)} = \begin{cases} i^{jm} Z^m X^j & \text{if } d = 2 \\ \omega^{-jm/2} Z^m X^j & \text{if } d \neq 2. \end{cases} \quad (2)$$

where $(j,m) \in \mathbb{Z}_d \times \mathbb{Z}_d$. **For N particules**, one takes the Kronecker product of qudit elements N times.

Stabilizer states are defined as eigenstates of the Pauli group.

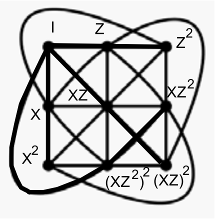
- Using **permutation groups**, we discover **minimal IC-POVMs** (i.e. whose rank of the Gram matrix is d^2) and with Hermitian angles $|\langle\psi_i|\psi_j\rangle|_{i\neq j} \in A = \{a_1, \ldots, a_l\}$, a discrete set of values of small cardinality l. A SIC is equiangular with $|A| = 1$ and $a_1 = \frac{1}{\sqrt{d+1}}$.
- The states encountered below are considered to live in a **cyclotomic field** $\mathbb{F} = \mathbb{Q}[\exp(\frac{2i\pi}{n})]$, with $n = \mathrm{GCD}(d, r)$, the greatest common divisor of d and r, for some r. The Hermitian angle is defined as $|\langle\psi_i|\psi_j\rangle|_{i\neq j} = \|(\psi_i, \psi_j)\|^{\frac{1}{\deg}}$, where $\|.\|$ means the field norm [3] of the pair (ψ_i, ψ_j) in $\mathbb{F}$ and deg is the degree of the extension $\mathbb{F}$ over the rational field $\mathbb{Q}$.
- For the IC-POVMs under consideration below, in dimensions $d = 3$, 4, 5, 6 and 7, one has to choose $n = 3$, 12, 20, 6 and 21 respectively, in order to be able **to compute the action of the Pauli group**. Calculations are performed with **Magma**.

[3] H. Cohen, A course in computational algebraic number theory (Springer, New York, 1996, p. 162).

The single qutrit (Hesse) SIC-POVM from permutations: 1

- The symmetric group S_3 contains the **permutation matrices** I, X and X^2 of the Pauli group, where $X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \equiv (2,3,1)$ and three **extra permutations** $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \equiv (2,3)$, $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \equiv (1,3)$ and $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv (1,2)$, that do not lie in the Pauli group but are parts of the Clifford group.
- Taking the **eigensystem of the latter matrices**, it is not difficult check that there exists two types of qutrit magic states of the form $(0,1,\pm 1) \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle \pm |2\rangle)$. Then, taking the action of the nine qutrit Pauli matrices, one arrives at the well known **Hesse SIC** (Bengtsson, 2010,Tabia, 2013, Hughston, 2007).

The single qutrit (Hesse) SIC-POVM from permutations: 2



Magic qutrit POVM's
(0,1,1) or (0,1,-1)

(a)

- The Hesse configuration resulting from the qutrit POVM. The lines of the configuration correspond to traces of triple products of the corresponding projectors equal to $\frac{1}{8}$ [for the state $(0,1,-1)$] and $\pm\frac{1}{8}$ [for the state $(0,1,1)$]. Bold lines are for commuting operator pairs.

IC-POVMs in dimensions 2 to 12

dim	magic state	$\lvert\langle\psi_i\vert\,\psi_j\rangle\rvert^2_{i\neq j}$	Geometry
2	$\lvert T\rangle$	$1/3$	tetrahedron
3	$(0,1,\pm 1)$	$1/4$	Hesse SIC
4	$(0,1,-\omega_6,\omega_6-1)$	$\{1/3,1/3^2\}$	**Mermin square***
5	$(0,1,-1,-1,1)$	$1/4^2$	Petersen graph
	$(0,1,i,-i,-1)$		
	$(0,1,1,1,1)$	$\{1/3^2,(2/3)^2\}$	
6	$(0,1,\omega_6-1,0,-\omega_6,0)$	$\{1/3,1/3^2\}$	Borromean rings
7	$(1,-\omega_3-1,-\omega_3,\omega_3,\omega_3+1,-1,0)$	$1/6^2$	unknown
8	$(-1\pm i,1,1,1,1,1,1,1)$	$1/9$	$[63_3]$ **Hoggar SIC***
9	$(1,1,0,0,0,0,-1,0,-1)$	$\{1/4,1/4^2\}$	$[9_3]$ **Pappus conf.***
12	$(0,1,\omega_6-1,\omega_6-1,1,1,$ $\omega_6-1,-\omega_6,-\omega_6,0,-\omega_6,0)$	8 values	Fig. 6

- Magic states of IC-POVMs in dimensions 2 to 12. *In dimensions 4, 8 and 9, a proof of the two-qubit, two-qutrit and three-qubit Kochen-Specker theorem follows from the IC-POVM.

A two-qubit IC-POVM from permutations and the Mermin square: 1

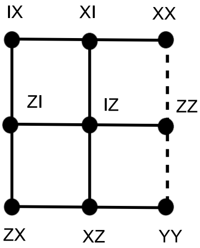
- From now we restrict to a **magic groups** (of gates showing one entry of 1 on their main diagonals). This only happens for a group isomorphic to the alternating group

$$A_4 \cong \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

  One finds magic states of type $(0,1,1,1)$ and $(0,1,-\omega_6,\omega_6-1)$, with $\omega_6 = \exp(\frac{2i\pi}{6})$.

- Taking the action of the 2**QB Pauli group on the latter type of state**, the corresponding pure projectors sum to 4 times the identity (to form a **POVM**) and are independent, with the pairwise distinct products satisfying the dichotomic relation $\text{tr}(\Pi_i\Pi_j)_{i\neq j} = |\langle\psi_i|\,\psi_j\rangle\,|^2_{i\neq j} \in \{\frac{1}{3}, \frac{1}{3^2}\}$. Thus the 16 projectors Π_i build an **asymmetric informationally complete** measurement not discovered so far.

A two-qubit IC-POVM from permutations and the Mermin square: 2



2QB IC-POVM : Mermin square

(b)

- The triple products of the four dimensional IC-POVM whose trace equal $\pm\frac{1}{27}$ and simultaneously equal plus or minus the identity matrix $\mathcal{I}$ ($-\mathcal{I}$ for the dotted line). This picture identifies to the well known Mermin square which allows a proof of the Kochen-Specker theorem.

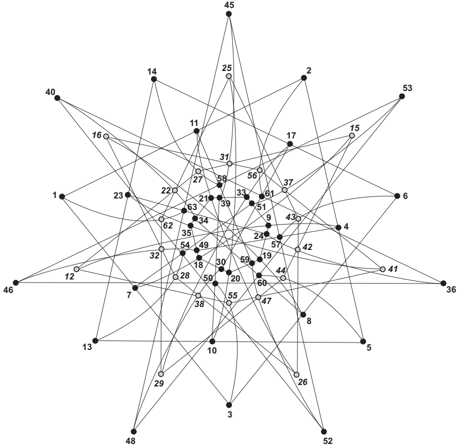
The three-qubit Hoggar SIC : 1

- In dimension $d = 8$, the **Hoggar SIC** [4] follows from the action of the three-qubit Pauli group on a fiducial state such as $(-1 \pm i, 1, 1, 1, 1, 1, 1, 1)$.
- Triple products are related to combinatorial designs. There are 4032 (resp. 16128) triples of projectors whose products have trace equal to $-\frac{1}{27}$ (resp. $\frac{1}{27}$). Within the 4032 triples, those whose product of projectors equal $\pm\mathcal{I}$ are organized into a configuration $[63_3]$ whose incidence graph kas automorphism group $G_2(2) = U_3(3) \rtimes \mathbb{Z}_2$ of order 12096. Two isospectral configurations of this type exist, one is the so-called **generalized hexagon** $GH(2,2)$ (also called split Cayley hexagon) and the other one is **its dual** (Frohard, 1994). These configurations are related to the 12096 Mermin pentagrams that build a proof of the **three-qubit Kochen-Specker theorem** [5]. From the structure of hyperplanes of our $[63_3]$ configuration, one learns that we are concerned with the dual of G_2.

[4] B. M. Stacey, Geometric and information-theoretic properties of the Hoggar lines, arxiv 1609.03075 [quant-ph].

[5] M. Planat, M. Saniga and F. Holweck, Distinguished three-qubit 'magicity' via automorphisms of the split Cayley hexagon, *Quant. Inf. Proc.* **12** 2535-2549 (2013).

The three-qubit Hoggar SIC: 2



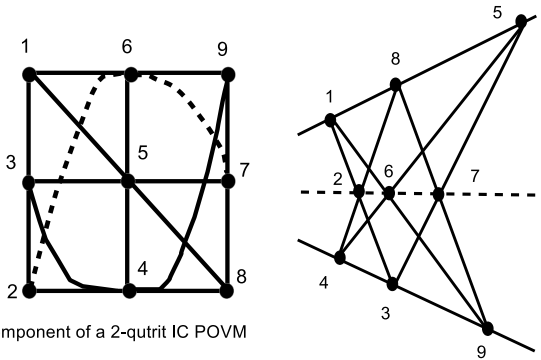
- The dual of the generalized hexagon $GH(2,2)$. Grey points have the structure of an embedded generalized hexagon $GH(2,1)$.

The two-qutrit IC-POVM: 1

- Let us consider a magic group isomorphic to $\mathbb{Z}_3^2 \rtimes \mathbb{Z}_4$ generated by two magic gates. One finds a few magic states such as $(1,1,0,0,0,0,-1,0,-1)$ that, not only can be used to generate a **dichotomic IC-POVM with distinct pairwise products** $|\langle\psi_i|\,\psi_j\rangle\,|^2$ equal to $\frac{1}{4}$ or $\frac{1}{4^2}$, but also show a quite simple organization of triple products.

  Defining lines as triple of projectors with trace $\frac{1}{8}$, one gets a configuration of type $[81_3]$ that split into **nine disjoint copies of the Pappus configuration** $[9_3]$.

The two-qutrit IC-POVM: 2



component of a 2-qutrit IC POVM

- One component of the two-qutrit IC-POVM. The points are labeled in terms of the two-qutrit operators $[1,2,3,4,5,6,7,8,9] = [I \otimes Z, I \otimes XZ, I \otimes (XZ^2)^2, Z \otimes I, Z \otimes X, Z \otimes X^2, Z^2 \otimes Z^2, Z^2 \otimes (XZ)^2, Z^2 \otimes XZ^2]$, where X and Z are the qutrit shift and clock operators.

The two-qutrit IC-POVM: 3

- The Pappus $[9_3]$ may be used to provide an **operator proof of 2QT KS theorem** (in the same spirit than the one derived for 2QB and 3QB). On one hand, **every operator O can be assigned a value $\nu(O)$ which is an eigenvalue of O**, that is 1 or $\pm\omega_3$. Taking the product of eigenvalues over all operators on a line and over all nine lines, one gets ± 1 since $1^3 = 1$, $(\pm\omega_3)^3 = \pm 1$ and every assigned value occurs three times. The whole product is ± 1.
- On the other hand, the operators on a line of Pappus do not necessarily commute but their product is $\mathcal{I} = I \otimes I$, $\omega_3\mathcal{I}$ or $\omega_3^*\mathcal{I}$, depending on the order of operators in the product. Taking the ordered triples $[1,6,9]$, $[9,7,8]$, $[2,4,8]$, $[1,3,2]$, $[8,5,1]$, $[3,5,7]$, $[3,4,9]$, $[4,5,6]$ and $[2,6,7]$, the triple product of these operators from left to right equals $\mathcal{I}$ **except for the dotted line** where it is $\omega_3\mathcal{I}$.
- Thus the product law $\nu(\Pi_{i=1}^9 O_i) = \Pi_{i=1}^9[\nu(O_i)]$ is violated. **The left hand side equals ω_3 while the right hand side equals** ± 1. The lines are not defined by mutually commuting operators so that one cannot arrive at a 2QT KS proof based on vectors instead of operators.

Conclusion and perspectives

- Many asymmetric IC-POVMs built thanks to the action of the Pauli group on appropriate permutation generated magic/fiducial states.
- The relationship between such (S)IC-POVMs and the Kochen-Specker theorem
- Perspectives: one can start from the permutation representation of the modular group $PSL(2,\mathbb{Z})$ to relate such problems (and the KS-theorem) to modular forms and elliptic curves (current work).

Appendix: 1. Near (and generalized) polygons

- A **near polygon** is a connected partial linear space S, with the property that given a point x and a line L, there always exists a unique point on L nearest to x.
- A generalized polygon (or generalized n-gon) is an incidence structure between a discrete set of points and lines whose incidence graph has diameter n and girth $2n$ [6].

  The definition implies that a generalized n-gon cannot contain i-gons for $2 \leq i < n$ but can contain ordinary n-gons.

  A generalized polygon of order (s, t) is such that every line contains $s + 1$ points and every point lies on $t + 1$ lines.

  A projective plane of order n is a generalized 3-gon. The generalized 4-gons are the generalized quadrangles. Generalized 6-gons, 8-gons, etc are **hexagons, octagons,** etc.

  According to Feit-Higman theorem, finite generalized n-gons with $s > 1$ and $t > 1$ may exist only for $n \in \{2, 3, 4, 6, 8\}$

[6] The **diameter** of a graph is the distance between its furthest points. The **girth** is the shortest path from a vertex to itself.

Geometry [7]	l	u	l/u	$\log_2(h)$	Remark
$GQ(2,1)$	6	5	1.2	4	Mermin square
$GQ(2,2)$	15	3	5	5	two-qubit commutation
$GQ(2,4)$	45	5	9	6	black-hole/qubit analogy
$GH(2,1)$	14	2	7	8	in the dual of $GH(2,2)$ [8]
$GO(2,1)$	30	2	15	16	in $GO(2,4)$ [9]
$GH(2,2)$	63	3	**21**	14	3-qubit contextuality
dual of $GH(2,2)$	63	4	**15.75**	14	id

Geometric contextuality measure l/u (l the number of lines and u the number of them with mutually commuting cosets) for a few generalized polygons compared $\log_2(h)$ with h the number of geometric hyperplanes within the selected geometry.

[7] A Tits generalized polygon (or generalized n-gon) is a point-line incidence structure whose incidence graph has diameter n and girth $2n$

[8] D. Frohard and, P. Johnson, Geometric hyperplanes in generalized hexagons of order $(2,2)$, *Comm. Alg.* **22** 773 (1994).

[9] B. De Bruyn, The uniqueness of a certain generalized octagon of order $(2,4)$, Preprint 2011.