*Article*

# The Poincaré Half-Plane for Informationally-Complete POVMs

**Michel Planat** ᴵᴰ

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

**Abstract:** It has been shown in previous papers that classes of (minimal asymmetric) informationally-complete positive operator valued measures (IC-POVMs) in dimension $d$ can be built using the multiparticle Pauli group acting on appropriate fiducial states. The latter states may also be derived starting from the Poincaré upper half-plane model $\mathbb{H}$. To do this, one translates the congruence (or non-congruence) subgroups of index $d$ of the modular group into groups of permutation gates, some of the eigenstates of which are the sought fiducials. The structure of some IC-POVMs is found to be intimately related to the Kochen–Specker theorem.

**Keywords:** informationally-complete POVMs; modular group; quantum computing

**PACS:** 03.67.-a; 03.65.Wj; 02.20.-a; 03.65.Fd; 03.65.Aa; 02.10.Ox; 03.65.Ud; 03.67.Lx

**MSC:** 11F06; 20H05; 81P50; 81P68; 81P13; 81P45; 20B05

## 1. Introduction

*Nulle parole ne trouve une branche où se poser (No words find a branch where to land [1]).*

Out of nothing I have created a strange new universe wrote Janos Bolyai to his father in 1823. Additionally, W. K. Clifford wrote, What Vesalius was to Galen, what Copernicus was to Ptolemy, Lobachevsky was to Euclid [2]. Half a century later, Felix Klein published the Erlangen program making explicit the relationship of all geometries to projective geometry via their own groups of symmetries. To illustrate the rise of non-Euclidean ideas in this epoch, let us quote a few words of M. Pasch to F. Klein in 1891 [3]:

*I am also late in thanking you for sending your essay on non-Euclidean geometry from last year... I also agree with most of what you say in the last two pages of your essay. The content of the axioms comes from observations (intuition as an internal activity is based on remembering what has been observed); the concepts used in the axioms, however, are inexact, and thus so are the axioms themselves. These latter can, however, only be used purely logically if they are presented as being exact. By further working on the axioms and seeking geometric propositions, we commonly make use of figures, either by drawing them or by 'imagining' them... The consideration must be possible even without the figures, in other words: that which is derived from the figures must already be contained in the axioms, for otherwise the axioms are not complete.*

Pasch's axiom (of plane geometry) was used by Hilbert to complete Euclid's axioms. It is related to Pasch's configuration of points and lines (in projective geometry). Incidence geometry, born at the time of Pappus of Alexandria, developed with Desargues (1591–1661), Jacob Steiner (1796–1863), Thomas Kirkman (1806–1895), Gino Fano (1871–1952), David Hilbert (1862–1943) and, more recently, with Jacques Tits (1930–) and Francis Buekenhout (1937–).

What kind of relation does quantum mechanics maintain with projective geometry? The superposition of states in Hilbert space $\mathcal{H}$ is linear but, due to the probability interpretation of the wave function, a state is not a single vector, but a ray, i.e., a one-dimensional subspace of $\mathcal{H}$. As a result, the space of rays is not a linear, but a projective space. It is known from Wigner's theorem (1931) that the realization of symmetries for pure states of a quantum mechanical system is (up to a scalar) a unitary or anti-unitary transformation [4,5]; see also [6–8] for the relation to positive operator valued measures (POVMs). It is worthwhile to point out that many of the basic configurations of incidence geometry are associated to the commutation relations between Hermitian operators in the (generalized) Pauli group [9]. Some projective configurations also occur in the structure of informationally-complete positive operator valued measures (IC-POVMs) [10,11].

Section 2 is a prolegomenon to the modular group $\Gamma$, its finite index subgroups $\Gamma_s$ and the connection to permutation gates considered in previous papers [10,11]. Then, one deals with the concept of IC-POVMs, the relation to the Pauli group and the occurrence of the Kochen–Specker theorem. The main goal of the paper, worked out in Section 3, is the derivation of "modular" ICs that follow from the structure of $\Gamma$. In small dimensions $d < 10$, triple products of projectors encapsulate recognizable finite geometries (already described in [11]), some of them related to the Kochen–Specker theorem. For $10 \leq d \leq 27$, many ICs may be constructed thanks to appropriate subgroups $\Gamma_s$. A summary of the results is in Table 1.

## 2. Prolegomenon about $\Gamma$ and Its Relation to IC-POVMs

### 2.1. The Modular Group $\Gamma$

The facts of science and, à fortiori, its laws are the artificial work of the scientist; science therefore can teach us nothing of the truth; it can only serve us as rule of action [12].

A standard non-Euclidean geometry consists of the Poincaré hyperbolic plane $\mathbb{H} = \{x, y \in \mathbb{R} | y > 0\}$ whose symmetry group is the projective (special) linear group $L = PSL(2, \mathbb{R})$ of real Möbius transformations of $\mathbb{H}$. A discrete subgroup of $L$ is called a Fuchsian group with the modular group $\Gamma = PSL(2, \mathbb{Z})$ as the most celebrated example. Important mathematical objects are the moduli space of elliptic curves, which is the quotient space $\mathbb{H}/\Gamma$, and modular forms that map pairs of points of $\mathbb{H}$ up to a weight factor and are also related to elliptic curves (via the 1995 modularity theorem) [13].

The modular group $\Gamma$ acts discontinuously on the extended upper half-plane $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \infty$, i.e., for each $z \in \mathbb{H}^*$, there exists a neighborhood of $z$ with no other element in the orbit of $z$. Thus, $\Gamma$ tessellates $\mathbb{H}^*$ with infinitely many copies of the fundamental domain $\mathcal{F} = \{z \in \mathbb{H}$ with $|z| > 1$, $\Re(z) < \frac{1}{2}\}$. The modular group $\Gamma$ is generated by two transformations $S_\Gamma : z \to -\frac{1}{z}$ and $T_\Gamma : z \to z + 1$. It can also be represented as the two-generator free group $G = \langle e, v | e^2 = v^3 = 1 \rangle$ using the variable change $e = S_\Gamma$ and $v = S_\Gamma T_\Gamma$.

Some finite index subgroups of $\Gamma$, called congruence subgroups, are obtained by fixing congruence relations on the entries of elements of $\Gamma$. The principal congruence subgroup of level $N$ of $\Gamma$ is the normal subgroup $\Gamma(N) = \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) | a, d = \pm 1 \mod N$ and $b, c = 0 \mod N$ whose index is $n^3 \Pi_{p|N}(1 - \frac{1}{p^2})$, $p$ a prime number. Another important subgroup of $\Gamma$ is the congruence subgroup $\Gamma_0(N)$ of level $N$ defined as the subgroup of upper triangular matrices with entries defined modulo $N$. The index of $\Gamma_0(N)$ is the Dedekind psi function $\psi(N)$. More generally, a congruence subgroup $\Gamma_c$ contains $\Gamma(N)$ for some $N$, and the level of $\Gamma_c$ is the smallest positive $N$ such that $\Gamma(N) \supseteq \Gamma_c$.

**Table 1.** A summary of the subgroups of the modular group $\Gamma$ (Column 2) allowing the construction of informationally-complete positive operator valued measures (IC-POVMs) in the corresponding dimension (Column 1). When non-congruence (denoted NC), the signature NC $(g, N, \nu_2, \nu_3, [c_i^{W_i}])$ is made explicit. Column 3 shows the minimal number of pairwise distinct products needed (denoted PP).

| Dim | Subgroups of $\Gamma$ Leading to an IC-POVM | PP | Geometry |
|---|---|---|---|
| 2 | none | 1 | tetrahedron [14] |
| 3 | $\Gamma_0(2)$ | 1 | Hesse SIC [15] |
| 4 | under 2QB Pauli group $\Gamma_0(3), 4A^0$ | 2 | $GQ(2,2)$ |
| 5 | $5A^0$ | 1 | Petersen graph |
| 6 | $\Gamma', \Gamma(2), 3C^0, \Gamma_0(4), \Gamma_0(5)$ | 2 | Borromean ring |
| 7 | $7A^0$ NC$(0, 6, 1, 1, [1^16^1])$ none | 2 2 1 | Figure 5b [11] |
| 8 | none under 3QB, 8-dit, 4-dit-QB Pauli group | 1 | Hoggar SIC [11,16] |
| 9 | under 2QT Pauli group NC$(0, 8, 3, 0, [1^18^1])$ NC$(0, 9, 1, 3, [9^1])$ | 2 3 | $(3 \times 3)$-grid, Pappus $[81_8, 216_3]$ |
| 10 | $5C^0$ | 5 | |
| 11 | $11A^0$ | 3 | $[11_3]$ |
| 12 | under 2QB-QT Pauli group $10A^1$ NC $(0, 8, 4, 0, [4^18^1])$ NC$(0, 8, 4, 0, [4^18^1])$ | 5 5 6 | $K(3,3,3,3)$ Hesse $(\times 16)$ $[48_7, 112_3]$ |
| 12 | under 12-dit Pauli group $8A^1$, NC$(0, 8, 4, 0, [4^18^1])$ | 11,7 | |
| 13 | NC$(0, 6, 1, 1, [1^16^2])$ | 4 | |
| 14 | $7C^0$, NC$(0, 6, 0, 2, [1^16^2])$, $14A^1$ | 12,5,6 | |
| 15 | $5E^0$, NC$(0, 6, 3, 0, [3^16^2])$, $15A^1$, $10B^1$ | 5,4,10,3 | |
| 16 | none under 4QB and 2 4-dit Pauli group | | |
| 18 | under 18-dit or 2QT-QB Pauli group $\Gamma_0(10)$, NC$(1, 8, 0, 0, [2^18^2])$ | 7,5 | |
| 19 | NC$(0, 6, 1, 1, [1^16^3])$ | 3 | |
| 21 | NC$(0, 6, 3, 0, [3^16^3])$, NC$(0, 6, 1, 0, [1^12^16^3])$ NC$(0, 14, 7, 0, [7^114^1])$, NC$(0, 8, 3, 0, [1^14^18^2])$ | 4 59,4 | |
| 24 | none under 3QB-QT Pauli group | | |
| 24 | under 24-dit Pauli group $24A^1$, NC$(2, 12, 0, 0, [12^2])$, $20B^1$, $12F^1$ NC$(0, 6, 2, 0, [3^26^3])$, NC$(1, 8, 0, 0, [4^28^2])$ $21A^2$, $24A^1$ | 40,56,40,30 8,7 23,60 | |
| 25 | under 25-dit Pauli group NC$(0, 10, 5, 1, [5^110^2])$ | 15 | |
| 27 | under 3QT Pauli group NC$(0, 6, 1, 0, [1^12^16^4])$, NC$(0, 8, 3, 0, [1^12^18^3])$ | 4 | Pappus |

Important geometric invariants of a finite index subgroup $\Gamma_s$ of $\Gamma$ (either congruence or not) are the genus, the structure of elliptic points and that of cusps (parabolic points) [17]. These concepts

are defined below. A fundamental domain $\mathbb{F}_s$ of $\Gamma_s$ in the upper half-plane $\mathbb{H}$ is such that for any $z \in \mathbb{H}$, there is a unique $\gamma \in \Gamma_s$ such that $\gamma(z) \in \mathbb{F}_s$. The subgroup $\Gamma_s$ acts discontinuously on the extended upper half-plane $\mathbb{H}^*$ and tessellates it with infinitely many copies of $\mathbb{F}_s$. Fixed points in $\mathbb{H}$ are elliptic points. An elliptic point of $\Gamma_s$ is a transformation $\gamma \in \Gamma_s$ such that $\gamma(z) = z$ and $\gamma \neq \pm I$, where $I$ is the identity matrix. Elliptic points of $\Gamma_s$ satisfy $|\text{tr}(\gamma)| < 2$, and their order can only be two or three. Their numbers are denoted $\nu_2$ and $\nu_3$, respectively. A cusp of $\Gamma_s$ is a fixed point of the extended upper-half plane $\mathbb{H}^*$ such that $|\text{tr}(\gamma)| = 2$. It can be shown that the action of $\Gamma_s$ partitions $\mathbb{Q} \cup \infty$ into equivalence classes where $q_1 \sim q_2$ if $q_1 = \gamma q_2$ for some $\gamma \in \Gamma_s$. These equivalence classes correspond to the cusps of $\Gamma_s$, and the widths of the cusps are the ratios between the orders of $\text{Stab}_{\Gamma(q)}$ and $\text{Stab}_{\Gamma_s(q)}$. The level of $\{q\}$ is the least common multiple of the cusp widths of $\Gamma$. The structure of cusps is denoted $[\cdots c_i^{w_i} \cdots]$ with $c_i$ the number of cusps of width $W_i$. In Table 1, the signature of a non-congruence subgroup $\Gamma_s$ is represented as NC $(g, N, \nu_2, \nu_3, [\cdots c_i^{w_i} \cdots])$. If the subgroup of $\Gamma$ is a congruence subgroup $\Gamma_c$, the geometric invariants are available in [18]. To conclude this subsection, a Farey symbol for $\Gamma_s$ is a certain finite sequence of rational numbers (they are fractions representing vertices of a fundamental domain of $\Gamma_s$) together with pairing information for the edges between the vertices [17]. This concept is needed to construct the fundamental domain of a finite index subgroup of $\Gamma$.

Using methods developed in [17,18] and implemented in the Sage software [19], one can represent a subgroup $G$ of $\Gamma$ either through the permutation representation $P$ of the cosets of $G$ in $\Gamma$ (by making use of the Coxeter–Todd algorithm) or through the modular representation of $P$. The permutation representation of a finite index subgroup of the two-generator free group is known as a dessin d'enfant [9–11]. The modular picture is possible here since $G$ is a subgroup of $\Gamma$. Doing this, one arrives at the unexplored relationship of permutation gates of quantum computing, informationally-complete POVMs [10,11] and the aforementioned modular objects.

## 2.2. Minimal Informationally-Complete POVMs and the Pauli Group

In QBism , all the personalist Bayesian properties of probability theory carry over to quantum states; that is, quantum states, like probabilities, are valuations of belief for future experiences [20].

The paper is a continuation of [11] while restricting to permutation gates stemming from subgroups of $\Gamma$. Our interest is still the search for minimal informationally-complete (IC)-POVMs derived from appropriate fiducial states under the action of the (generalized) Pauli group.

A POVM is a collection of positive semi-definite operators $\{E_1, \ldots, E_m\}$ that sum to the identity. In the measurement of a state $\rho$, the $i$-th outcome is obtained with a probability given by the Born rule $p(i) = \text{tr}(\rho E_i)$. 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 $\text{tr}(\Pi_i \Pi_j)$ is precisely $d^2$.

A SIC-POVM (the S means symmetric) obeys the remarkable relation [21]:

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

that allows the explicit recovery of the density matrix as in [22] (Equation (29)). The fiducial states for SIC-POVMs are quite complicated to derive (e.g., [23] for an update), and one must work very hard to find anything simple about them [24].

In this paper, we discover minimal IC-POVMs (i.e., whose rank of the Gram matrix is $d^2$) and with Hermitian angles $\left| \langle \psi_i | \psi_j \rangle \right|_{i \neq j} \in A = \{a_1, \ldots, a_l\}$, 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 $n = \text{GCD}(d, r)$, the greatest common divisor of $d$ and $r$, for some $r$. The Hermitian angle is defined as $\left| \langle \psi_i | \psi_j \rangle \right|_{i \neq j} = \left\| (\psi_i, \psi_j) \right\|^{\frac{1}{\deg}}$, where $\|.\|$ means the field norm [25] (pp. 162) of the pair $(\psi_i, \psi_j)$ in $\mathbb{F}$ and deg is the degree of the extension $\mathbb{F}$ over the rational field $\mathbb{Q}$ [11].

We construct the relevant IC-POVMs using the covariance with respect to the generalized Pauli group. Let $d$ be a prime number; the qudit Pauli group is generated by the shift and clock operators as follows:

$$X \left| j \right\rangle = \left| j + 1 \mod d \right\rangle$$
$$Z \left| j \right\rangle = \omega^j \left| j \right\rangle \tag{2}$$

with $\omega = \exp(2i\pi/d)$ a $d$-th root of unity. In dimension $d = 2$, $X$ and $Z$ are the Pauli spin matrices $\sigma_x$ and $\sigma_z$. For $N$ particles, one takes the Kronecker product of qudit elements $q$ times.

Stabilizer states are defined as eigenstates of the Pauli group.

### 2.3. The Single Qubit SIC-POVM

The covariance property under the Pauli group can be illustrated in the two-dimensional case. One can start with the qubit fiducial/magic state $\left| T \right\rangle = \cos(\beta) \left| 0 \right\rangle + \exp\left(\frac{i\pi}{4}\right) \sin(\beta) \left| 1 \right\rangle$, $\cos(2\beta) = \frac{1}{\sqrt{3}}$, employed for universal quantum computation [14]. It is defined as the $\omega_3 = \exp\left(\frac{2i\pi}{3}\right)$—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 $\left| T \right\rangle$ of the four Pauli gates $I$, $X$, $Z$ and $Y$, the corresponding (pure) projectors $\Pi_i = \left| \psi_i \right\rangle \left\langle \psi_i \right|$, $i = 1, \dots, 4$, sum to twice the identity matrix, thus building a POVM, and the pairwise distinct products satisfy $\left| \left\langle \psi_i \right| \psi_j \right\rangle |^2 = \frac{1}{3}$. The four elements $\Pi_i$ form the well-known two-dimensional SIC-POVM ([21], Section 2).

### 2.4. The Kochen–Specker Theorem

Humans are rats who themselves construct the labyrinth they propose to escape (Rats qui construisent eux-mêmes le labyrinthe dont ils se proposent de sortir.) [26].

In a nutshell, the measured value of a quantum observable sometimes depends on which other mutually-compatible measurements might be performed. This leads to the concept of quantum contextuality. State-independent contextuality is often formulated in terms of the Kochen–Specker (KS) theorem because this theorem is able to guarantee the non-existence of non-contextual hidden variable theories, at least for dimension $d \geq 3$. A non-coloring KS proof consists of a finite set of projectors that cannot be assigned truth values (one for true, zero for false) in such a way that (i) one member of each complete orthonormal basis is true and (ii) no two orthogonal (that is, mutually-compatible) projectors are both true; see [27–29] and the references therein. Remarkably, it will be shown that subsets of projectors within the IC-POVMs below may sometimes be used to derive proofs of KS theorem (in Dimensions 4, 8 and 9). Contextuality and negativity of the Wigner function happen to play a fundamental role in universal schemes of quantum computation (e.g., [10,20,30,31]).

## 3. Permutation Gates from $\Gamma$, Fiducial States and Informationally-Complete Measurements

In all of the paper, we restrict to IC-POVMs that are built from subgroups of the modular group $\Gamma$ (in contrast to [11], where more general subgroups of the two-generator free groups were also considered).

Using the function "G.aspermutation.group()" in Sage [19], the permutation representation of the group $G$ is converted into that of the relevant subgroup $\Gamma_s$ of $\Gamma$. If $\Gamma_s$ is congruence, it can be identified in the Cummins–Pauli table [18] from its features, e.g., the genus $g$, the level $N$, the number of elliptic points of order two $\nu_2$, the number of elliptic points of order three $\nu_3$, the number of cusps $c$ of widths $W$, as well as the fractions of the Farey symbol.

### 3.1. The Three-Dimensional Hesse SIC

The only permutation group that can be used to build a three-dimensional IC-POVM (here, an SIC) is the symmetric group $S_3 = \langle e, v \rangle$ with generators $e = (2,3) \equiv \left( \begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix} \right)$ and $v = (1,2,3) \equiv \left( \begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix} \right)$, made explicit in terms of the (Index 3) permutation representation and the corresponding permutation gate. Using Sage and the table of congruence subgroups [18], it is straightforward to recognize that

$\Gamma_s = \Gamma_0(2)$, whose fundamental domain is pictured in Figure 1b. In this particular case, $\nu_2 = 1$ (the elliptic point at $z = \frac{1}{2}(1+i)$ is denoted by the symbol *), $\nu_3 = 0$, the cusps are at zero and $\infty$ and the fractions are at zero and one. The subgroup $\Gamma_s = \Gamma_0(2)$ is generated by two transformations $S_{\Gamma_s} : z \to \frac{z-1}{2z-1}$ and $T_{\Gamma_s} : z \to z+1$.

The eigenstates of the permutation matrices in $S_3$ can serve as fiducial states for an IC-POVM as qutrits in the classes $(0, 1, \pm 1) \equiv \frac{1}{\sqrt{2}}(|1\rangle \pm |2\rangle)$. Taking the action of the the nine qutrit Pauli matrices, one arrives at the well-known Hesse SIC. The Hesse SIC is illustrated in Figure 1c: the lines of the configuration correspond to projectors whose traces of triple products equal $\pm\frac{1}{8}$ [32], ([11], Figure 1a). Instead of labeling coordinates as projectors, one labels them with the qutrit operators acting on the fiducial state.
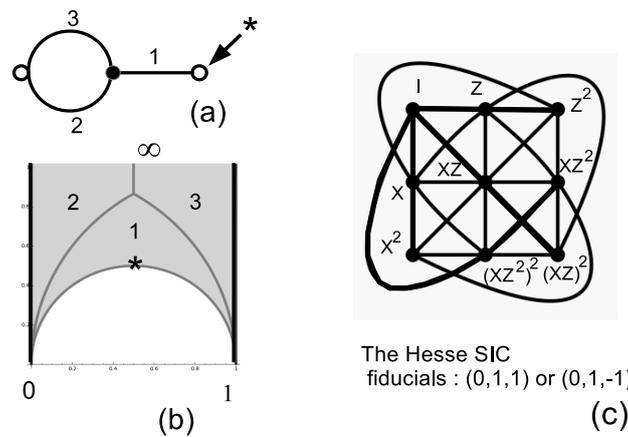


**Figure 1.** Representation of $S_3 \cong \Gamma_0(2)$ as a dessin d'enfant (**a**) and as the tiling of the fundamental domain (the two thick vertical lines have to be identified) (**b**). The character * denotes the unique elliptic point (of order two). The resulting Hesse SIC-POVM (symmetric informationally-complete positive operator valued measure) is in (**c**).

### 3.2. The Two-Qubit IC-POVM

The smaller permutation group that can be used to build a four-dimensional IC-POVM is the alternating group $A_4 = \langle e, v \rangle$ with generators $e = (1,2)(3,4) \equiv \left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right)$ and $v = (2,3,4) \equiv \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{smallmatrix}\right)$, made explicit in terms of the (Index 4) permutation representation and the corresponding permutation gate. Using Sage and the table of congruence subgroups [18] one recognizes that $\Gamma_s = \Gamma_0(3)$, whose fundamental domain is pictured in Figure 2b. In this particular case, $\nu_2 = 0$, $\nu_3 = 1$ (the elliptic point at $\frac{1}{2}(1 + \frac{i}{\sqrt{3}})$ is denoted by the symbol *), the cusps are at zero and $\infty$ and the fractions are at zero and one. The subgroup $\Gamma_s = \Gamma_0(3)$ is generated by two transformations $S_{\Gamma_s} : z \to \frac{z-1}{3z-2}$ and $T_{\Gamma_s} : z \to z+1$.

The joined eigenstates of the commuting permutation matrices in $S_3$ that can serve as fiducial states for an IC-POVM are of the form $(0, 1, -\omega_6, \omega_6 - 1) \equiv \frac{1}{\sqrt{3}}(|01\rangle - \omega_6 |10\rangle + (\omega_6 - 1) |11\rangle)$, with $\omega_6 = \exp(\frac{2i\pi}{6})$. Taking the action of the two-qubit Pauli group on the latter type of state, the corresponding pure projectors sum to four-times the identity (to form a POVM) and are independent, with the pairwise distinct products satisfying the dichotomic relation $\mathrm{tr}(\Pi_i \Pi_j)_{i \neq j} = |\langle \psi_i | \psi_j \rangle|^2_{i \neq j} \in \{\frac{1}{3}, \frac{1}{3^2}\}$. Thus, the 16 projectors $\Pi_i$ build an asymmetric informationally-complete POVM (see also [11], Section 2).

The organization of triple products of projectors whose trace is constant (that is, equal to $\frac{1}{9}$ or $\pm\frac{1}{27}$) is that of the generalized quadrangle of order two $GQ(2,2)$ (see [33] and the references therein

for more on this concept), as shown in Figure 2c. Simultaneously, the two-qubit operators labeling the vertices of $GQ(2,2)$ are such that the product of operators on a line of $GQ(2,2)$ equals the identity matrix or its negative. By restricting to triples of projectors whose trace is $\pm\frac{1}{27}$, one identifies the standard Mermin square in Figure 2d that is known to allow an operator proof of the Kochen–Specker theorem (e.g., [28]).

Finally, let us observe that the group $S_4 = \langle (1,2), (2,3,4) \rangle$ may also be used to built the two-qubit IC-POVM as above. It corresponds to the congruence subgroup $4A^0$ in the Cummins–Pauli table: it is of Level 4, with $\nu_2 = 2$, $\nu_3 = 1$ and a single cusp at $\infty$.
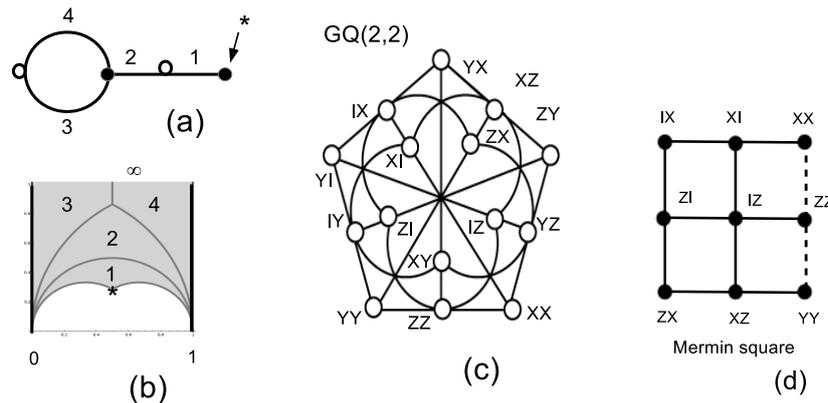


**Figure 2.** Representation of $A_4 \cong \Gamma_0(3)$ as a dessin d'enfant (**a**) and as the tiling of the fundamental domain (the two thick vertical lines have to identified) (**b**). The character * denotes the unique elliptic point (of order three). The organization of triple products of projectors leads to the generalized quadrangle $GQ(2,2)$ pictured in (**c**) whose subset is the Mermin square (**d**). Traces of triple products for rows (respectively columns) of the Mermin square equal $-\frac{1}{27}$ (respectively $\frac{1}{27}$).

### 3.3. The Five-Dimensional Equiangular IC-POVM

There is just one subgroup of Index 5 (up to conjugation) of the two-generator free group isomorphic to $\Gamma$. The organization of cosets defines the alternating group $A_5 = \langle e, v \rangle$ with generators $e = (1,2)(4,5)$ and $v = (2,3,4)$. Using Sage and the table of congruence subgroups [18], one recognizes that $\Gamma_s$ is the congruence subgroup $5A^0$ of Level 5 whose fundamental domain is pictured in Figure 3b.

There is one single elliptic point of order two, two elliptic points of order three denoted by the symbol *, one cusp at $\infty$ and two fractions at $-1$ and zero. The subgroup $\Gamma_s = 5A^0$ is generated by three transformations $z \to -\frac{z+2}{z+1}$, $z \to -\frac{2z+1}{3z+1}$ and $z \to \frac{1}{1-z}$. Fixed points of such transformations correspond to elliptic points of order two at $z = -1 + i$ and order three at $z = \frac{1+i\sqrt{3}}{2}$ and $z = -\frac{1}{2} + \frac{i}{2\sqrt{3}}$.

The joined eigenstates of the commuting permutation matrices in $A_5$ that can serve as fiducial states for an IC-POVM are of type $(0,1,1,1,1)$ and $(0,1,-1,-1,1)$. The latter type allows one to construct IC-POVM's such that the pairwise distinct products satisfy $|\langle \psi_i | \psi_j \rangle|^2 = \frac{1}{4^2}$, that is the POVM is equiangular with respect to the field norm defined in the Introduction. The first type of magic state is dichotomic with values of the products $\frac{1}{4^2}$ and $(\frac{3}{4})^2$. The trace of pairwise products of (distinct) projectors is not constant. For example, with the state $(0,1,-1,-1,1)$, one gets a field norm equiangular IC-POVM in which the trace is trivalued: it is either $1/16$ or $(7 \pm 3\sqrt{5})/32$.

Let us concentrate on the equiangular POVM. Traces of triple products with constant value $-\frac{1}{4^3}$ define lines organized into a geometric configuration of type $(25_{12}, 100_3)$. Lines of the configuration have one or two points in common. The two-point intersection graph consists of 10 disjoint copies of the Petersen graph. One such Petersen graph is shown in Figure 3c; the vertices of the graph correspond to the lines, and the edges correspond to the one-point intersection of two lines. As before, the labeling is in terms of the operators acting on the magic state.
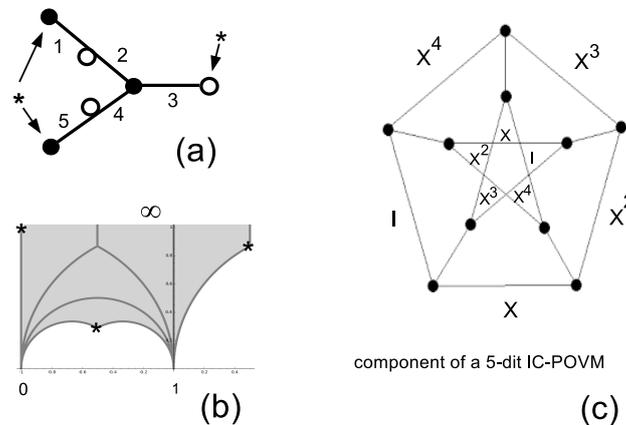
**Figure 3.** Representation of $A_5 \cong 5A^0$ as a dessin d'enfant (**a**) and as the tiling of the fundamental domain (**b**). The character * denotes the two elliptic points of order three. (**c**) A one-point intersection graph organizing the lines of the five-dit equiangular informationally-complete positive operator valued measure (IC-POVM) defined from the triple products of constant trace $-\frac{1}{4^3}$.

## 3.4. The Six-Dimensional IC-POVM

One finds five distinct permutation groups of Index 6 corresponding to subgroups of $\Gamma$ that lead to a six-dimensional IC-POVM. Fiducial states are of type $(0, 1, \omega_6 - 1, 0, -\omega_6, 0)$ already found in [11] with $\mathrm{tr}(\Pi_i \Pi_j)_{i \neq j} = |\langle \psi_i | \psi_j \rangle|^2_{i \neq j} = \frac{1}{3}$ or $\frac{1}{3^2}$.
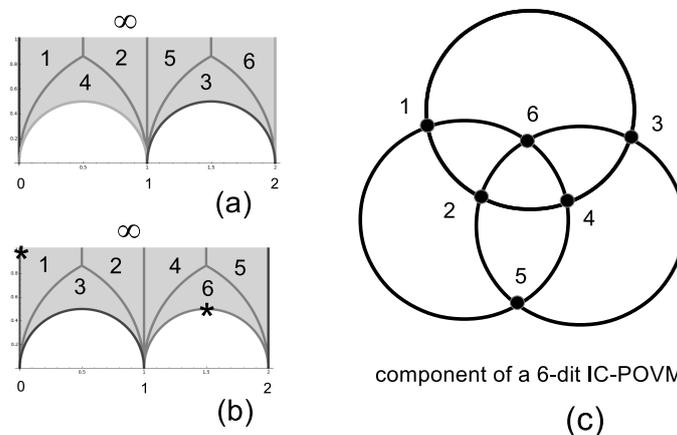


**Figure 4.** (**a**) Fundamental domain for the genus 1 group $\Gamma'$; (**b**) fundamental domain for the genus 0 group $6A^1$; the symbol * points out the two elliptic points of order two; (**c**) a basic piece of the six-dit IC-POVM with fiducial state of type $(0, 1, \omega_6 - 1, 0, -\omega_6, 0)$ obtained through the action of Pauli operators 1–6: the lines correspond to four-tuple products of projectors with constant trace $\frac{1}{9}$ and simultaneously of products equal to $\pm \mathcal{I}$. There are two disjoint copies looking like Borromean rings with points as $[1 \dots 6] = [\mathcal{I}, ZX^3, Z^2, Z^3X^3, Z^4, Z^5X^3]$ (for lines with projector products $-I$) and $[1 \dots 6] = [X^4, Z, Z^2X^3, Z^3, Z^4X^3, Z^5]$ (for lines with projector products $I$).

The five permutation groups under question are the cyclic group $\mathbb{Z}_6$ leading to congruence subgroups $\Gamma'$ and $\Gamma(2)$, the alternating group $A_4$ leading to the congruence subgroup $3C^0$ [18] and the symmetric group $S_4$ leading to the congruence subgroups $\Gamma_0(4)$ and $\Gamma_0(5)$. Fundamental domains for $\Gamma'$ and $3C^0$ are shown in Figure 4a,b, respectively.

For a six-dimensional IC-POVM, one discovers a quite simple geometry sustaining the four-tuple products of projectors having constant trace $\frac{1}{9}$ and simultaneously having products of corresponding operators on a line equal to $\pm I$. It consists of two disjoint copies (corresponding to lines whose product of projectors equal $-I$ and $I$, respectively) looking like Borromean rings, as shown in Figure 4.

### 3.5. Seven-Dimensional IC-POVMs

Seven-dimensional IC-POVMs with bivalued pairwise products $\left|\langle \psi_i | \psi_j \rangle\right|^2_{i \neq j}$ are found starting from permutation groups isomorphic to $\mathbb{Z}_7 \rtimes \mathbb{Z}_6$ or $PSL(2,7)$, respectively. The first permutation group corresponds to a non-congruence subgroup. The fiducials of the IC are of type $(0, 1, 1, 1, \pm 1, \pm 1, \pm 1)$ or $(0, 1, -\omega_3 - 1, \omega_3, 1, -\omega_3 - 1, \omega_3)$. The second permutation group corresponds to the congruence subgroup $7A^0$ [18]. The fiducials of the IC are of type $(1, 0, 0, 0, 1, \pm 1, \pm 1)$ or $(1, 0, 0, 0, i, i, 1)$.

The fundamental domain for the group $7A^0$ is shown in Figure 5a. The geometry of IC triple products is quite complex, but one building block may be identified as shown in Figure 5b (only for ICs with non-complex entries in their fiducial).



(a)

(b)
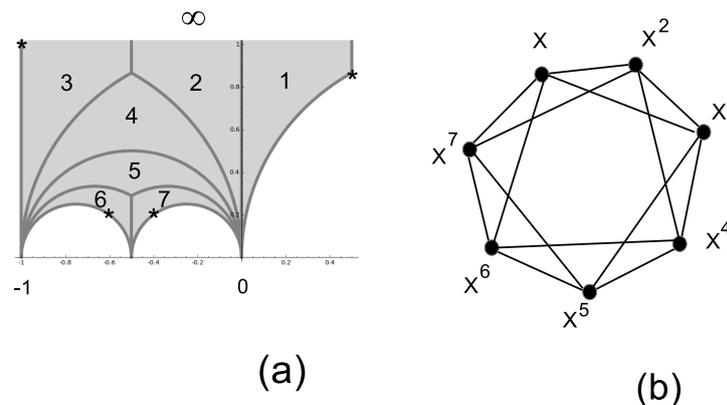
**Figure 5.** (**a**) Fundamental domain for the group $7A^0$; (**b**) a basic component associated with a bivalued seven-dimensional IC-POVM.

It may be reminded that an equiangular (with respect to the cyclotomic field norm) seven-dimensional IC-POVM exists. It is obtained thanks to the group $\mathbb{Z}_7 \rtimes \mathbb{Z}_6$ (in a non-modular representation) using magic permutations [11]. A fiducial such as $(1, -\omega_3 - 1, -\omega_3, \omega_3, \omega_3 + 1, -1, 0)$ does the job with $\left|\langle \psi_i | \psi_j \rangle\right|^2_{i \neq j} = \frac{1}{6^2}$.

### 3.6. The Three-Qubit Hoggar SIC

The approach based on permutation groups fails to identify any IC-POVM; see [16] for details about the geometry of the Hoggar SIC in relation to its covariance under the three-qubit Pauli group. A noticeable result is that the three-qubit SIC embeds the dual of the generalized hexagon $GH(2,2)$ [11,16] (Figure 3). The latter geometry is connected to the eight-dimensional Kochen–Specker theorem.

### 3.7. Nine-Dimensional IC-POVMs

The smallest permutation group isomorphic to a subgroup of $\Gamma$ and useful to build a nine-dimensional IC-POVM is $P = \langle (1,2,3)(4,5,6)(7,8,9), (3,4)(5,7)(8,9) \rangle \cong \mathbb{Z}_3^2 \rtimes (\mathbb{Z}_2 \rtimes S_4)$. The corresponding fundamental domain is shown in Figure 6a, the subgroup is non-congruence and contains three elliptic points of order two at $i$, $2 + i$ and $(1 + i)/2$ and two cusps at $\frac{3}{2}$ and $\infty$. The related IC-POVM has bi- or three-valued distinct pairwise products. Let us choose the fiducial state for the bivalued case as $(1, 0, 0, 0, \pm 1, 0, 0, \pm 1, 1, 0)$. For the state with positive entries and traces of

triple products equal to $-\frac{1}{8}$, the geometry consists of six copies of a $3 \times 3$ grid, as shown on Figure 6b. The products of the observables on a row or a column of the grid equal one, $\omega_3$ or $\omega_3^2$. For the state with positive and negative entries and traces of triple products equal to $\frac{1}{8}$, the geometry consists of nine copies of the Pappus configuration, as shown in Figure 6c. It allows the proof of the 2-qutrit Kochen–Specker theorem [11] (Section 2.7 and Figure 5).
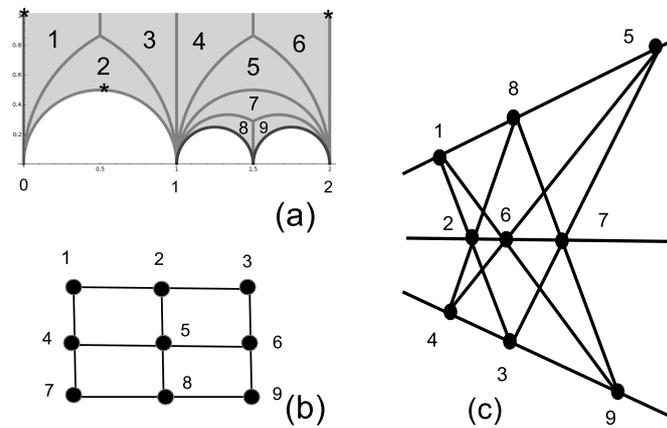


**Figure 6.** (**a**) Fundamental domain for the non congruence subgroup of $\Gamma$ associated with the group $\mathbb{Z}_3^2 \rtimes (\mathbb{Z}_2 \rtimes S_4)$. (**b**) A basic component (a $(3 \times 3)$-grid) in the geometry of the bivalued nine-dimensional IC-POVM with fiducial $(1, 0, 0, 0, 1, 0, 1, 1, 0)$. Vertices of the grid for observables are the two-qutrit observables $[1, \cdots, 9] = [I \otimes X, I \otimes XZ, I \otimes XZ^2, Z \otimes X, Z \otimes XZ, Z \otimes XZ^2, Z^2 \otimes X, Z^2 \otimes XZ, Z^2 \otimes XZ^2]$. (**c**) A basic component (a Pappus configuration) in the geometry of the bivalued nine-dimensional IC-POVM with fiducial $(1, 0, 0, 0, -1, 0, -1, 1, 0)$. The points are $[1, \cdots, 9] = [I \otimes Z, I \otimes XZ, I \otimes (XZ^2)^2, Z \otimes I, Z \otimes X, Z \otimes X^2, Z^2 \otimes Z^2, Z^2 \otimes (XZ)^2, Z^2 \otimes XZ^2]$.

A trivalued IC-POVM follows from the permutation group of order 504 that is also non-congruence. The fiducial is of type $(0, 1, 1, 1, 1, 1, 1, 1, 1)$.

It is useful to remind that a group generated by two magic permutations and isomorphic to $\mathbb{Z}_3^2 \rtimes \mathbb{Z}_4$ has been used to construct a bivalued IC-POVM starting from a fiducial of type $(1, 1, 0, 0, 0, 0, -1, 0, -1)$ [11]. Noticeably, It contains the Pappus configuration in the organization of its triple products.

### 3.8. Higher Dimensional IC-POVMs

IC-POVMs found in dimension $d$ higher than nine are summarized in the second half of Table 1. The minimal number of pairwise products needed increases with $d$ (as in Column 3), and the subgroup $\Gamma_s$ occurring in the construction is quite often non-congruence (as expressed in Column 2). The symmetry underlying triple products of projectors is not simple and not easily recognizable. We could not find (modular group based) IC-POVMs in dimensions $d = 8, 16, 17, 22, 23$. In Dimension 24, the found ICs are covariant under the 24-dit Pauli group, not under the 3*QB*-*QT* group. Finally, in Dimension 27, one finds a four-valued IC-POVM, covariant under the 3QT Pauli group, whose structure of the triple products consists of 81 copies of the Pappus configuration.

Table 1 summarizes the results obtained so far.

## 4. Conclusions

It would be nice if we could design a virtual reality in Hyperbolic Space, and meet each other there [34].

The continuing search of mathematical structures governing the weirdness of quantum theory is catalyzed by applications. A universal quantum computer needs non-stabilizer states, i.e., states that are not eigenstates of a Pauli group. The finding of distillable qubit magic states in [14] prompted us to

pass to higher dimensions with the methods of permutation theory [10]. It was soon observed that an interesting subset of magic states could be seen as fiducials for minimal IC-POVMs of the corresponding dimension [11]. Now, the present work connects universal quantum computing, IC-POVMs, quantum contextuality and the subgroups of finite index $\Gamma_s$ of the modular group $\Gamma$. This allows one to see the magic/fiducial states arising from appropriate permutation gates in the new language of fundamental domains and their copies under the discontinuous action of $\Gamma_s$. Thus and unexpectedly, a short circuit occurs between $\Gamma$ and quantum theory that has not been investigated so far. The group $\Gamma$ is the starting point of the modularity theorem that connects elliptic curves over the rationals and modular forms. A jewel of mathematics is tethered to our best physical theory.

**Conflicts of Interest:** The author declares no conflict of interest.

## References

1. Ghesquier, M.-F. *A Hauteur d'Ombre*; Cardère: Avignon, France, 2014; p. 57.
2. Lobachevsky N.I. *Pangeometry*; European Mathematical Society: Zurich, Switzerland, 2010; ISBN 9783037190876.
3. Schlimm, D. The correspondence between Moritz Pasch and Felix Klein. *Hist. Math.* **2013**, *40*, 183–202.
4. Keller, K.J.; Papadopoulos, N.A.; Reyes-Lega, A.F. On the realizations of symmetries in quantum mechanics. *arXiv* **2008**, arXiv:0712.0997.
5. Freed, D.S. On Wigner's theorem. *Geom. Topol. Monogr.* **2012**, *18*, 83–89.
6. Słomczyński, W.; Szymusiak, A. Highly symmetric POVMs and their informational power. *Quant. Inf. Process.* **2016**, *15*, 565–606.
7. Dang, H.B. Studies of Symmetries That Give Special Quantum States the "Right to Exist". Ph.D. Thesis, University of Waterloo, Waterloo, ON, Canada, 11 August 2015.
8. Chien, T.Y.; Waldron, S. Nice error frames, canonical abstract error groups and the construction of SICs. *Linear Algebra Appl.* **2017**, *516*, 93–117.
9. Planat, M.; Zainuddin, H. Zoology of Atlas-Groups: Dessins D'enfants, Finite Geometries and Quantum Commutation. *Mathematics* **2017**, *5*, 6.
10. Planat, M.; Ul Haq, R. The magic of universal quantum computing with permutations. *Adv. Math. Phys.* **2017**, *217*, 5287862.
11. Planat, M.; Gedik, Z. Magic informationally complete POVMs with permutations. *R. Soc. Open Sci.* **2017**, *4*, 170387.
12. Poincaré, H. *La Valeur de la Science (The Value of Science)*; Flammarion: Paris, France, 1905; p. 214. (In French)
13. Diamond, F.; Shurman, J. *A First Course in Modular Forms*; Springer: New York, NY, USA, 2005.
14. Bravyi, S.; Kitaev, A. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A* **2005**, *71*, 022316.
15. Bengtsson, I. From SIC's and MUBs to Eddington. *J. Phys. Conf. Ser.* **2010**, *254*, 012007.
16. Stacey, B.C. Geometric and information-theoretic properties of the Hoggar lines. *arxiv* **2016**, arxiv:1609.03075.
17. Kurth, C.A.; Long, L. Computations with finite index subgroups of $PSL(2, \mathbb{Z})$ using Farey symbols. In *Advances in Algebra and Combinatorics*; Shum, K.P., Zelmanov, E., Zhang, J., Li, S., Eds.; World Scientific: Singapore, 2008; pp. 225–242.
18. Cummins, C.J.; Pauli, S. Congruence Subgroups of PSL(2,Z) of Genus Less than or Equal to 24. *Exp. Math.* **2003**, *12*, 243–255.
19. Stein, W.A.; Abbott, T.; Abshoff, M.; Ajanki, A.; Albrecht, M.; Alexander, N.; Allombert, B.; Van Andel, E.; Andrus, I.; Angulo, P.; et al. *Sage Mathematics Software*, Version 6.4.1; The Sage Development Team: Washington, WA, USA, 2014. Available online: http://www.sagemath.org (accessed on 1 January 2017).
20. DeBrota, J.B.; Fuchs, C.A. Negativity bounds for Weyl-Heisenberg quasiprobability representations. *Found. Phys.* **2017**, *47*, 1009–1030.

21. Renes, J.M.; Blume-Kohout, R.; Scott, A.J.; Caves, C.M. Symmetric informationally complete quantum measurements. *J. Math. Phys.* **2004**, *45*, 2171–2180.
22. Fuchs, C.A. On the quantumness of a Hibert space. *Quant. Inf. Comput.* **2004**, *4*, 467–478.
23. Appleby, M.; Chien, T.Y.; Fammia, S.; Waldron, S. Constructing exact symmetric informationally complete measurements from numerical solutions. *arxiv* **2017**, arxiv:1703.05981.
24. Bengtsson, I. The number behind the simplest SIC-POVM. *Found Phys.* **2017**, *47*, 1031–1041.
25. Cohen, H. *A Course in Computational Algebraic Number Theory*; Springer: New York, NY, USA, 1996.
26. Queneau, R.; Le Lionnais, F. Wikimedia. Available online: https://en.wikipedia.org/wiki/oulipo (accessed on 1 January 2017).
27. Cabello, A. A proof with 18 vectors of the Bell–Kochen–Specker theorem. In *New Developments on Fundamental Problems in Quantum Physics*; Ferrero, M., van der Merwe, A., Eds.; Kluwer Academic: Dordrecht, The Netherlands, 1997; pp. 59–62.
28. Planat, M. On small proofs of Bell-Kochen–Specker theorem for two, three and four qubits. *Eur. Phys. J. Plus* **2012**, *127*, 86.
29. Pavičić, M. Arbitrarily exhaustive hypergraph generation of 4-, 6-, 8-, 16-, and 32-dimensional quantum contextual sets. *Phys. Rev. A* **2017**, *95*, 062121.
30. Delfosse, N.; Guerin, P.A.; Bian, J.; Raussendorf, R. Wigner function negativity and contextuality in quantum computation on rebits. *Phys. Rev. X* **2015**, *5*, 021003.
31. De Silva, N. Logical paradoxes in quantum computation. *arxiv* **2017**, arxiv:1709.00013.
32. Tabia, G.N.M.; Appleby, D.M. Exploring the geometry of qutrit space using symmetric informationally complete probabilities. *Phys. Rev. A* **2013**, *88*, 012131.
33. Planat, M. Pauli graphs when the Hilbert space dimension contains a square: Why the Dedekind psi function? *J. Phys. A Math. Theor.* **2011**, *44*, 045301.
34. Knuth, D. Π M & Epsilon J. S. Frame Talk, MathFest. Avaliable online: http://sites.math.rutgers.edu/~zeilberg/quotes.html (accessed on 1 January 2017).