An operational link between MUBs and SICs

Roberto Beneduci*
Dipartimento di Matematica, Università della Calabria, Cosenza, and INFN gruppo collegato Cosenza, Cosenza, Italy

Thomas J Bullock† and Paul Busch‡
Department of Mathematics, University of York, York, UK

Claudio Carmeli§
D.I.M.E., Università di Genova, Savona, Italy

Teiko Heinosaari¶
Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku, Finland

Alessandro Toigo**
Dipartimento di Matematica, Politecnico di Milano, Milano, and I.N.F.N., Sezione di Milano, Italy
(Dated: September 25, 2013)

We exhibit an operational connection between mutually unbiased bases and symmetric informationally complete positive operator-valued measures. Assuming that the latter exists, we show that there is a strong link between these two structures in all prime power dimensions. We also demonstrate that a similar link cannot exist in dimension 6.

I. INTRODUCTION

The existence of *symmetric informationally complete positive operator valued measures* (SIC POVMs, or simply SICs) in arbitrary dimensions and the existence of complete systems of $d+1$ mutually unbiased bases (MUBs) in complex Hilbert spaces of dimensions d other than prime power have remained unsolved despite much effort expended on them over the last ten years or so. Connections with finite geometries have been exhibited for both SICs and MUBs, including the intriguing fact that the relevant geometries for either of them are equivalent (where they exist) [1, 2]. The construction schemes proposed so far for SICs and MUBs are essentially mathematically motivated and based on combinatorial, group theoretic, algebraic or finite geometric structures [3–14].

Here we elucidate a physically motivated connection between SICs and MUBs, which emerges quite naturally in some respects. Our main tools will be the generalisation of a SIC POVM into a *SIC system* and of MUBs into *mutually unbiased POVMs*.

The basic idea is easily established by considering the qubit case: there a SIC is found to be a natural joint observable of three POVMs that are smearings of three mutually unbiased binary observables. It turns out that these POVMs have a similar relation as mutually unbiased bases and they will therefore be referred to as mutually unbiased POVMs. Characteristic properties of mutually unbiased POVMs arising as marginals of SICs in dimension d are established; these properties will be referred to as SIC compatibility conditions. We show that whenever a complete system of mutually unbiased commutative POVMs is obtained from a SIC, it is possible to extract a complete system of MUBs.

The condition for a SIC possessing $d+1$ mutually unbiased POVMs as marginals is found to be equivalent to there being $d-1$ orthogonal Latin squares of size d. Conversely, given a complete system of mutually unbiased POVMs for dimension d, a system of operators can be canonically constructed such that it contains these mutually unbiased POVMs as marginals whenever there are $d-1$ orthogonal Latin squares of order d. This system possesses all properties of a SIC except, possibly, positivity. Such a collection of operators will be called a SIC system. For each complete MUB system there is an infinite variety of SIC systems. It is an open problem to identify SICs among them where they exist.

Finite covariant phase space observables constitute a concrete application of the general framework sketched above. Here, we recall that finite covariant phase space observables are POVMs based on finite phase spaces (see [6]) and are covariant with respect to the discrete Weyl-Heisenberg representation acting on a $d = p^n$-dimensional Hilbert space (with p a prime number different from 2, and n a positive integer). We show that every finite covariant phase space observable admits $d+1$ mutually unbiased and commutative marginal POVMs that are smearings of $d+1$ MUBs. As an application of the general results developed in the first part of the paper, in Theorem 5 we then characterize SIC covariant phase space observables in terms of a particular property of their mutually unbiased marginal POVMs.

* roberto.beneduci@unical.it
† tjb525@york.ac.uk
‡ paul.busch@york.ac.uk
§ claudio.carmeli@gmail.com
¶ teiko.heinosaari@utu.fi
** alessandro.toigo@polimi.it

Our construction scheme for MUBs from SICs and vice versa may be seen as a possible realisation of the construction scheme outlined by Wootters [2]; the equivalence of the associated finite geometries pointed out there is found here to systematically underpin the SIC-MUB bridge via the marginality relation employed.

II. MUBS, SICS, AND THEIR CONNECTION IN $d = 2$

A. MUBs and their generalisation

Throughout the paper the underlying complex Hilbert space will be of dimension d and denoted $\mathcal{H}_d$ or occasionally $\mathbb{C}^d$. A basic structure to be used is a function $k \mapsto \mathsf{E}(k)$ from some finite set Ω of outcomes to the set of positive operators on $\mathcal{H}_d$ with the property that $\sum_k \mathsf{E}(k) = I$, the identity operator on $\mathcal{H}_d$. This kind of function determines a *positive operator valued measure*, in short, POVM. We refrain from using the appropriate measure theoretic language and simply refer to E as a POVM. If the elements of a POVM are projections we will call E a projection valued, or spectral, measure (PVM).

We begin by recalling the basic definition.

Definition 1. A family of orthonormal bases $\{\varphi_i^k\}_{i=0}^{d-1}$, $k = 1, 2, \ldots, n$ of a d-dimensional Hilbert space $\mathcal{H}_d$ are said to be *mutually unbiased* if, for any i, j,

$$\left|\langle\varphi_i^k|\varphi_j^\ell\rangle\right|^2 = \frac{1}{d}\left(1 - \delta_{k\ell}\right) + \delta_{k\ell}\delta_{ij}. \tag{1}$$

Let us note that if $\{\varphi_j^1\}$ and $\{\varphi_k^2\}$ are mutually unbiased orthonormal bases, then $\{\alpha_j\varphi_j^1\}$ and $\{\beta_k\varphi_k^2\}$ are also mutually unbiased for all complex numbers $\alpha_j, \beta_k \in \mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}$. Mutual unbiasedness is thus actually a property of the corresponding projections. Namely, define $\mathsf{P}^1(j) = |\varphi_j^1\rangle\langle\varphi_j^1|$ and $\mathsf{P}^2(k) = |\varphi_k^2\rangle\langle\varphi_k^2|$. Then (1) translates into

$$\mathrm{tr}\left[\mathsf{P}^1(j)\mathsf{P}^2(k)\right] = 1/d\,. \tag{2}$$

We will say that a family of PVMs whose elements satisfy (2) are mutually unbiased. Actually, from this we see that mutual unbiasedness admits a direct generalisation to all d-outcome POVMs.

Definition 2. Let J be an index set and $\{\mathsf{E}^j \mid j \in J\}$ a set of POVMs, with each E^j being based on a space I_j, where $|I_j| = d$. We say that the POVMs E^j, $j \in J$, are *mutually unbiased (MU)* if

$$\mathrm{tr}\left[\mathsf{E}^j(i_j)\mathsf{E}^k(i_k)\right] = 1/d$$

for all $j, k \in J$ with $j \neq k$, and $i_j \in I_j$, $i_k \in I_k$.

It is known that there are at most $d + 1$ mutually unbiased bases (MUBs) in $\mathcal{H}_d$ [16] and that sets of three MUBs can be constructed in any dimension [15]. If d is a prime power, that is, $d = p^n$ for some prime number p and $n \geq 1$, then $d + 1$ MUBs can be constructed in $\mathcal{H}_d$ [16]. However, for values of d that are not prime powers, this limit does not seem to be reached. For example, there is extensive numerical evidence suggesting that in $d = 6$ no set of three MUBs may be extended to a set with more MUBs [17].

B. SICs and their generalisation

Definition 3. A POVM G, with d^2 outcomes, acting on $\mathcal{H}_d$ is *symmetric informationally complete* (SIC POVM or simply SIC) if

$$\mathrm{tr}\left[\mathsf{G}(k)\mathsf{G}(\ell)\right] = \frac{1}{d^2(1+d)} \qquad \forall k \neq \ell, \tag{3}$$

$$\mathrm{tr}\left[\mathsf{G}(k)^2\right] = \frac{1}{d^2} \qquad \forall k\,. \tag{4}$$

It follows from this definition that

$$\mathrm{tr}\left[\mathsf{G}(k)\right] = \sum_\ell \mathrm{tr}\left[\mathsf{G}(k)\mathsf{G}(\ell)\right] = \frac{1}{d} \quad \forall k\,. \tag{5}$$

This, together with (4), implies that for each k, $d\mathsf{G}(k)$ is a rank-1 projection.

A SIC POVM G is automatically informationally complete, meaning that no two states give the same expectations for all $\mathsf{G}(k)$. This property follows from the fact that the operators $\mathsf{G}(k)$ form a basis of the vector space $\mathcal{L}(\mathcal{H}_d)$ of linear operators on $\mathcal{H}_d$, which can be shown directly from the definition or obtained as a consequence of the following interesting lemma [18].

Lemma 1. *Let G be a SIC on $\mathcal{H}_d$. Then the d^2 operators*

$$d\mathsf{G}(k) - tI\,, \quad \textit{where} \quad t = \frac{1}{d}\left(1 - \sqrt{\frac{1}{d+1}}\right), \tag{6}$$

form an orthogonal basis with respect to the Hilbert-Schmidt inner product in $\mathcal{L}(\mathcal{H}_d)$.

Proof. Consider $k \neq \ell$, then

$$\mathrm{tr}\left[(d\mathsf{G}(k) - tI)(d\mathsf{G}(\ell) - tI)\right] = dt^2 - 2t + \frac{1}{d+1} = 0$$

since it is easily verified that the above value of t is a root of this polynomial. □

The existence of a SIC POVM has been proved analytically for a number of low-dimensional cases [13, 19, 20] and numerically verified (as of 2010) up to the dimension 67 [13].

Since the existence of SIC POVMs in an arbitrary dimension is an open problem, we find it useful to introduce the following generalisation. We emphasize, however, that unlike the previous definitions this one has only mathematical motivation.

Definition 4. A collection of selfadjoint operators $\{\mathsf{G}(i)\}_{i=0}^{d^2-1}$ on $\mathcal{H}_d$ that satisfiy the SIC conditions (3)-(4), and the normalisation $\sum_i \mathsf{G}(i) = I$, is called a *SIC system.*

Note that positivity of the $\mathsf{G}(i)$'s is not required in the definition of a SIC system.

C. The SIC-MUB connection in $\mathcal{H}_2$

We show how a complete set of MUBs can be extracted from a SIC POVM in the case of a qubit system. A SIC G consists of four positive rank-1 operators

$$\mathsf{G}(k) = \frac{1}{4}(I + \boldsymbol{s}_k \cdot \boldsymbol{\sigma}), \tag{7}$$

where $k \in \mathbb{Z}_4$, $\|\boldsymbol{s}_k\| = 1$, and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector whose elements are the three Pauli matrices. The SIC condition reads

$$\mathrm{tr}\,[\mathsf{G}(i)\mathsf{G}(j)] = \frac{1}{12} = \frac{1}{8}(1 + \boldsymbol{s}_i \cdot \boldsymbol{s}_j)$$

that is,

$$\boldsymbol{s}_i \cdot \boldsymbol{s}_j = -\frac{1}{3} \quad \text{if} \quad i \neq j.$$

This means that the vectors $\boldsymbol{s}_i$ point to the vertices of a regular tetrahedron that lies on the surface of the Bloch sphere. In particular, their sum is the null vector, which ensures that $\sum_k \mathsf{G}(k) = I$.

One can form three pairs of binary marginal POVMs:

$$\begin{aligned} &\mathsf{E}^1(+) = \mathsf{G}(0) + \mathsf{G}(1), \quad \mathsf{E}^1(-) = \mathsf{G}(2) + \mathsf{G}(3), \\ &\mathsf{E}^2(+) = \mathsf{G}(0) + \mathsf{G}(2), \quad \mathsf{E}^2(-) = \mathsf{G}(1) + \mathsf{G}(3), \\ &\mathsf{E}^3(+) = \mathsf{G}(0) + \mathsf{G}(3), \quad \mathsf{E}^3(-) = \mathsf{G}(1) + \mathsf{G}(2). \end{aligned} \tag{8}$$

The positive operators $\mathsf{E}^k(\pm)$ are of the form

$$\mathsf{E}^k(\pm) = \frac{1}{2}(I \pm \boldsymbol{m}_k \cdot \boldsymbol{\sigma}). \tag{9}$$

where

$$\boldsymbol{m}_k := \frac{1}{2}(\boldsymbol{s}_0 + \boldsymbol{s}_k), \quad k = 1, 2, 3. \tag{10}$$

It is easily seen that

$$\boldsymbol{m}_k \cdot \boldsymbol{m}_\ell = \frac{1}{3}\delta_{k\ell}. \tag{11}$$

In order to diagonalize the $\mathsf{E}^k(\pm)$, we introduce the unit vectors $\boldsymbol{n}_k$ via $\boldsymbol{m}_k = \frac{1}{\sqrt{3}}\boldsymbol{n}_k \equiv \lambda \boldsymbol{n}_k$, and PVMs $\mathsf{P}^k(\pm) := \frac{1}{2}(I \pm \boldsymbol{n}_k \cdot \boldsymbol{\sigma})$. Then

$$\mathsf{E}^k(\pm) = \lambda \mathsf{P}^k(\pm) + \frac{1}{2}(1 - \lambda)I \tag{12}$$

$$= \frac{1}{2}(1 + \lambda)\mathsf{P}^k(\pm) + \frac{1}{2}(1 - \lambda)\mathsf{P}^k(\mp). \tag{13}$$

The POVMs E^k are thus found to arise as *smearings* of the PVMs P^k. Furthermore, one has

$$\mathrm{tr}\left[\mathsf{P}^k(\pm)\mathsf{P}^\ell(\pm)\right] = \frac{1}{2} \quad \text{for } k \neq \ell. \tag{14}$$

Hence, the three PVMs P^1, P^2 and P^3 are mutually unbiased.

In order to construct a SIC from a complete set of MUBs, one can reverse the steps taken in the above construction. Given a system of three MUBs, $\{\varphi_+^k, \varphi_-^k\}$, $k = 1, 2, 3$, define the PVMs $|\varphi_\pm^k\rangle\langle\varphi_\pm^k| =: \mathsf{P}^k(\pm) \equiv \frac{1}{2}(I \pm \boldsymbol{n}_k \cdot \boldsymbol{\sigma})$. Then apply the smearing according to (12) for some $\lambda \in [0, 1]$ to define the three POVMs E^k. We note that these POVMs are mutually unbiased independently of the value of λ, i.e.,

$$\mathrm{tr}\left[\mathsf{E}^k(\pm)\mathsf{E}^\ell(\pm)\right] = \frac{1}{2} \quad \text{for} \quad k \neq \ell\,. \tag{15}$$

Next, observe that the system of equations (8) can be solved; by summing all those triples of the positive operators $\mathsf{E}^k(\pm)$ that share one of the four operators $\mathsf{G}(i)$ and repeatedly using the fact that $\mathsf{G}(0)+\mathsf{G}(1)+\mathsf{G}(2)+\mathsf{G}(3) = I$ one finds:

$$\begin{aligned} \mathsf{E}^1(+) + \mathsf{E}^2(+) + \mathsf{E}^3(+) &= 2\mathsf{G}(0) + I, \\ \mathsf{E}^1(+) + \mathsf{E}^2(-) + \mathsf{E}^3(-) &= 2\mathsf{G}(1) + I, \\ \mathsf{E}^1(-) + \mathsf{E}^2(+) + \mathsf{E}^3(-) &= 2\mathsf{G}(2) + I, \\ \mathsf{E}^1(-) + \mathsf{E}^2(-) + \mathsf{E}^3(+) &= 2\mathsf{G}(3) + I. \end{aligned} \tag{16}$$

Thus, given the POVMs E^k, one can define operators $\mathsf{G}(i)$ as follows:

$$\begin{aligned} \mathsf{G}(0) &:= \frac{1}{2}\left(\mathsf{E}^1(+) + \mathsf{E}^2(+) + \mathsf{E}^3(+) - I\right), \\ \mathsf{G}(1) &:= \frac{1}{2}\left(\mathsf{E}^1(+) + \mathsf{E}^2(-) + \mathsf{E}^3(-) - I\right), \\ \mathsf{G}(2) &:= \frac{1}{2}\left(\mathsf{E}^1(-) + \mathsf{E}^2(+) + \mathsf{E}^3(-) - I\right), \\ \mathsf{G}(3) &:= \frac{1}{2}\left(\mathsf{E}^1(-) + \mathsf{E}^2(-) + \mathsf{E}^3(+) - I\right). \end{aligned} \tag{17}$$

Equations (17) entail immediately that the operators $\mathsf{G}(k)$ are selfadjoint and $\sum_k \mathsf{G}(k) = I$. But at this point, we need to choose $\lambda = 1/\sqrt{3}$ to make the operators $\mathsf{G}(k)$ positive. With that choice, it is straightforward to verify that G is actually a SIC.

III. FROM SICS TO MUBS

A. Marginals of a SIC POVM

We now consider the route of constructing (up to) $d+1$ MUBs from the d^2 elements of a SIC G on $\mathcal{H}_d$. First, note that any partition of G into disjoint bins constitutes a marginal POVM, where each of its positive operators is given as the sum of the SIC elements contained in one

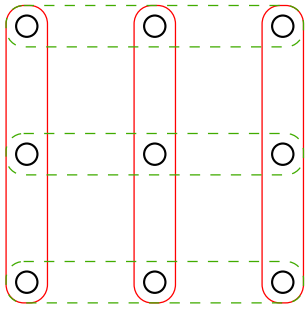

FIG. 1. Cartesian partitions. (Color online.)

of the bins. We will focus on partitions into d bins of size d; these have the property that the positive operators obtained by summing the SIC elements of each bin are unit trace.

Definition 5. A partition of a set of d^2 elements, $\{a_1, a_2, \ldots, a_{d^2}\}$, into d bins of d elements will be called a *d-partition.*

The structure of a d-partition will be required as it is the only kind of partition such that the positive operators obtained as the sums of the SIC elements within each bin have trace equal to 1. As we deal only with d-partitions we will also occasionally refer to them simply as *partitions.*

Clearly there exist many d-partitions. If we place the d^2 elements of $\{a_1, a_2, \ldots, a_{d^2}\}$ into a $d\times d$-array, then letting the rows be bins gives a first d-partition; and choosing the columns as bins gives a second (see Fig. 1). These two d-partitions, $\mathcal{P}^{(1)}$ and $\mathcal{P}^{(2)}$, which we shall refer to as the *Cartesian partitions*, have the following relevant property: any pair of bins, one from each of the two partitions, share exactly one element of the $d \times d$ array.

Definition 6. Any two distinct d-partitions, $\mathcal{P}^{(k)} = \{\mathcal{P}_1^{(k)} \ldots, \mathcal{P}_d^{(k)}\}$ and $\mathcal{P}^{(\ell)} = \{\mathcal{P}_1^{(\ell)}, \ldots, \mathcal{P}_d^{(\ell)}\}$, satisfying the condition that the cardinalities of all bin intersections $|\mathcal{P}_\mu^{(k)} \cap \mathcal{P}_\nu^{(\ell)}| = 1$ will be said to have (or share) the *1-overlap property.*

For a given bin $\mathcal{P}_\nu^{(k)}$ we define the trace-one operator

$$\mathsf{E}^k(\nu) = \sum_{\mathsf{G}(i)\in\mathcal{P}_\nu^{(k)}} \mathsf{G}(i). \tag{18}$$

For each d-partition $\mathcal{P}^{(k)}$ of G, the set of positive operators $\{\mathsf{E}^k(\nu)\}_{\nu=1}^d$ forms a marginal POVM E^k of the given SIC.

The following is an immediate consequence of the defining properties of a SIC.

Theorem 1. *Let G be a SIC, and let $\mathcal{P}^{(k)}$, $\mathcal{P}^{(\ell)}$ be two d-partitions of G with the 1-overlap property, with associated marginal POVMs E^k and E^ℓ. Then*

$$\mathrm{tr}\left[\mathsf{E}^k(\mu)\right] = 1, \quad \mu = 1, \ldots, d; \tag{19}$$

$$\mathrm{tr}\left[(\mathsf{E}^k(\mu))^2\right] = \frac{2}{d+1}, \quad \mu = 1, \ldots, d; \tag{20}$$

$$\mathrm{tr}\left[\mathsf{E}^k(\mu)\mathsf{E}^k(\nu)\right] = \frac{1}{d+1}, \quad \mu \neq \nu; \tag{21}$$

$$\mathrm{tr}\left[\mathsf{E}^k(\mu)\mathsf{E}^\ell(\nu)\right] = \frac{1}{d}, \quad \mu, \nu = 1, \ldots, d \quad \textit{for } k \neq \ell. \tag{22}$$

Proof. The trace-1 property is immediate.

$$\mathrm{tr}\left[\left(\mathsf{E}^k(\nu)\right)^2\right] = \sum_{\mathsf{G}(i)\in\mathcal{P}_\nu^{(k)}} \mathrm{tr}\left[(\mathsf{G}(i))^2\right] + \sum_{\substack{\mathsf{G}(i),\mathsf{G}(j)\in\mathcal{P}_\nu^{(k)} \\ i\neq j}} \mathrm{tr}\left[\mathsf{G}(i)\mathsf{G}(j)\right] = \frac{2}{d+1};$$

$$\mathrm{tr}\left[\mathsf{E}^k(\nu)\mathsf{E}^k(\mu)\right] = \sum_{\mathsf{G}(i)\in\mathcal{P}_\nu^{(k)}} \sum_{\mathsf{G}(j)\in\mathcal{P}_\mu^{(k)}} \mathrm{tr}\left[\mathsf{G}(i)\mathsf{G}(j)\right] = \frac{d^2}{d^2(d+1)} = \frac{1}{d+1} \quad \text{where } \mu \neq \nu;$$

$$\begin{aligned}\mathrm{tr}\left[\mathsf{E}^k(\nu)\mathsf{E}^\ell(\mu)\right] =& \mathrm{tr}\left[\mathsf{G}\big(i(\nu,\mu)\big)^2\right] + \sum_{\substack{\mathsf{G}(n)\in\mathcal{P}_\nu^{(k)} \\ n\neq i(\nu,\mu)}} \sum_{\substack{\mathsf{G}(m)\in\mathcal{P}_\mu^{(\ell)} \\ m\neq i(\nu,\mu)}} \mathrm{tr}\left[\mathsf{G}(n)\mathsf{G}(m)\right] \\ &+ \sum_{\substack{\mathsf{G}(m)\in\mathcal{P}_\mu^{(\ell)} \\ m\neq i(\nu,\mu)}} \mathrm{tr}\left[\mathsf{G}\big(i(\nu,\mu)\big)\mathsf{G}(m)\right] + \sum_{\substack{\mathsf{G}(n)\in\mathcal{P}_\nu^{(k)} \\ n\neq i(\nu,\mu)}} \mathrm{tr}\left[\mathsf{G}\big(i(\nu,\mu)\big)\mathsf{G}(n)\right] \\ =& \frac{1+d-1}{d^2} = \frac{1}{d}, \quad \text{where } \nu \neq \mu.\end{aligned}$$

Here $\mathsf{G}\big(i(\nu,\mu)\big)$ is the SIC element for which $i(\nu,\mu)$ is the unique shared label in $\mathcal{P}_\nu^{(k)} \cap \mathcal{P}_\mu^{(\ell)}$. □

Remark 1. We note for later use that (22) implies (19) and (21) implies (20) due to the normalisation of the POVMs.

It is worth noting that the effects $\mathsf{E}^k(\mu)$ in the marginal POVMs E^k are linearly independent.

Proposition 1. *Let E^k be a POVM satisfying conditions (19)-(21). The effects $\mathsf{E}^k(1), \ldots, \mathsf{E}^k(d)$ are linearly independent.*

Proof. Let $Y_\nu := \mathsf{E}^k(\nu) - \frac{1}{d+1} I$, $\nu = 1, 2, \ldots, n$. By equations (19), (20) and (21),

$$\mathrm{tr}\left[Y_\nu \mathsf{E}^k(\mu)\right] = \begin{cases} \frac{1}{d+1} & \text{if} \quad \nu = \mu, \\ 0 & \text{if} \quad \nu \neq \mu. \end{cases}$$

Suppose that $\sum_{\mu=1}^n c_\mu \mathsf{E}^k(\mu) = 0$. Then,

$$\begin{aligned} 0 &= \mathrm{tr}\Big[Y_\nu \sum_{\mu=1}^n c_\mu \mathsf{E}^k(\mu)\Big] = \sum_{\mu=1}^n c_\mu \mathrm{tr}\left[Y_\nu \mathsf{E}^k(\mu)\right] \\ &= c_\nu \frac{1}{d+1}, \quad \nu = 1, \ldots, n, \end{aligned}$$

which implies $c_\nu = 0$ for all $\nu = 1, \ldots, n$. Hence the linear independence follows. □

Definition 7. We will say that a collection of d-outcome POVMs is *SIC-compatible* if they are marginals of a common SIC.

A collection of SIC-compatible POVMs is *jointly measurable* or *compatible*, in the probabilistic sense that the SIC constitutes a joint observable. This scenario constitutes a remarkably strong form of joint measurability: a set of n random variables with (say) d outcomes gives rise to d^n joint event combinations, so that normally one would have to construct a joint observable with d^n outcomes. In the present case one can have up to $d+1$ marginals but the SIC constitutes a joint observable for all of them with only d^2 outcomes.

Theorem 1 thus states significant necessary conditions for the SIC-compatibility of a collection of mutually unbiased POVMs. A point of significance is that the 1-overlap property postulated for the system of d-partitions is necessary for the resulting marginal POVMs to be mutually unbiased. This will be proven below.

B. More on the 1-overlap property

Lemma 2. *The number of d-partitions of d^2 elements sharing the 1-overlap property is at most $d+1$ and at least 3.*

Proof. Suppose there are n d-partitions of a label set $\{a_1, a_2, \ldots, a_{d^2}\}$. Consider all bins of the n partitions that contain element a_1, say, and denote them by $\mathcal{P}_1^{(k)}$, where $1 \leq k \leq n$; so $\mathcal{P}_1^{(k)} \cap \mathcal{P}_1^{(\ell)} = \{a_1\}$ for all $k \neq \ell$. Hence all other elements within these bins cannot be repeated. There are $d^2 - 1$ other elements in $\{a_2, a_3, \ldots, a_{d^2}\}$ remaining to be distributed over the $\mathcal{P}_1^{(k)}$, and each of these bins must contain another $d-1$ elements, so the number of partitions $n \leq (d^2-1)/(d-1) = d+1$.

Next, if the elements of $\{a_1, a_2, \ldots, a_{d^2}\}$ (or their labels, for simplicity) are arranged in a $d \times d$ array,

$$\begin{array}{ccc} 1 & \ldots & d \\ \vdots & \ddots & \vdots \\ (d-1)d+1 & \ldots & d^2 \end{array}$$

then, as noted after Definition 5, the Cartesian partitions of rows and columns, $\mathcal{P}^{(1)}$ and $\mathcal{P}^{(2)}$, are d-partitions that share the 1-overlap property. By choosing these Cartesian partitions first, we are now restricted in the construction of any further partition: in order to satisfy the 1-overlap property with respect to the Cartesian partitions, no bin, besides those in $\mathcal{P}^{(1)}$ and $\mathcal{P}^{(2)}$, can contain two elements from the same row or column within this array.

A third d-partition, $\mathcal{P}^{(3)}$, that shares the 1-overlap property with the two Cartesian partitions can be obtained as follows. Relabel the elements of the $d \times d$-array in matrix form, (a_{ij}). Let $\mathcal{P}_1^{(3)}$ be the bin consisting of the main left-to-right diagonal, $\mathcal{P}_1^{(3)} = \{a_{11}, a_{22}, \ldots, a_{dd}\}$. Now consider the $2(d-1)$ subsets of the array that are given by as many diagonals parallel to this main diagonal. Denote by S_{1j} the diagonal subsets starting with the elements a_{1j}, $j \geq 1$, and by $S_{d+2-i,1}$ those starting with a_{i1}, $i \geq 2$. Then the disjoint bins $\mathcal{P}_1^{(3)} = S_{11}$ and $\mathcal{P}_\nu^{(3)} = S_{1\nu} \cup S_{\nu 1}$, $\nu \geq 2$, form a d-partition that shares the 1-overlap property with $\mathcal{P}^{(1)}$ and $\mathcal{P}^{(2)}$. □

From now on, any partition said to share the 1-overlap property is immediately assumed to share it with respect to the Cartesian partitions.

We recall the definition of an important structure within combinatorics. A *Latin square of order d* is a $d \times d$ array A in which each point on A contains an element from a symbol set S, where $|S| = d$, such that each row and column within A contains every element from S. In other words, no column or row within A has repetition of any element from S.

Consider two Latin squares of order d with symbol sets S and T, and construct a $d \times d$ array of ordered pairs (s, t) placed at point (i, j) (where i and j are the respective row and column indices), where $s \in S$ is the element found at that point in the array in the first Latin square, and likewise $t \in T$ is the element found at that point in the array in the second Latin square. These two Latin squares are *mutually orthogonal* if every ordered pair (s, t) is unique, that is no two points in the array have the same ordered pair.

With these definitions at hand we obtain the following proposition. We note that the second part concerning

the connection with orthogonal Latin squares was noted and proven by Miklós Hartmann [21].

Proposition 2. *There is a one-to-one correspondence between the set of d-partitions $\mathcal{P}^{(k)}$ of a $d \times d$ array that share the 1-overlap property with both Cartesian partitions $\mathcal{P}^{(1)}$, $\mathcal{P}^{(2)}$ and the set of Latin squares of order d. Furthermore, two d-partitions with the 1-overlap property with respect to each other and the Cartesian partitions correspond to mutually orthogonal Latin squares.*

Proof. Consider a single partition $\mathcal{P}^{(k)}$ of a $d \times d$ array sharing the 1-overlap property with the Cartesian partitions. Each bin $\mathcal{P}^{(k)}_\nu$ can be viewed as a path through this array, and due to the disjoint nature of the bins no two paths intersect at any point. Since each point of the array belongs to a bin, it is incident with a unique path. Thus one can attach to each point the label of the path it belongs to; in other words, we have a mapping $(i,j) \mapsto \nu^{(k)}_{i,j}$ from point labels (i,j) to path labels $\nu^{(k)}_{i,j} \in \{1,\ldots,d\}$. In order to share the 1-overlap property with the Cartesian partitions, no bin/path $\mathcal{P}^{(k)}_\nu$ can contain more than one element from any column or row within this array, and this corresponds to having no paths which can move strictly vertically or horizontally at any point, nor can they return to a row or column they have already been incident on. This means that no value of $\nu^{(k)}_{i,j}$ may be repeated within any row or column in the $d \times d$ array $\{\nu^{(k)}_{i,j}\}$. In other words we have proved that the array $\{\nu^{(k)}_{i,j}\}$ is a Latin square.

Conversely any Latin square of order d induces a path labelling on the elements of the given $d \times d$ array, and it is immediate that the resulting paths form a partition that shares the 1-overlap property with the Cartesian partitions.

Consider now two partitions $\mathcal{P}^{(k)}, \mathcal{P}^{(\ell)}$ that share the 1-overlap property between each other and the Cartesian partitions. Since they share the 1-overlap property with the Cartesian partitions they both correspond to Latin squares of order d, which we denote by $\{\nu^{(k)}_{i,j}\}$ and $\{\nu^{(\ell)}_{i,j}\}$ respectively. If we consider the $d \times d$ array $\{(\nu^{(k)}_{i,j}, \nu^{(\ell)}_{i,j})\}$, the 1-overlap property implies that the ordered pairs $(\nu^{(k)}_{i,j}, \nu^{(\ell)}_{i,j})$ are distinct for all i,j; i.e., the Latin squares are orthogonal. Indeed, if it were that $(\nu^{(k)}_{i,j}, \nu^{(\ell)}_{i,j}) = (\nu^{(k)}_{n,m}, \nu^{(\ell)}_{n,m})$, then we would have two paths, $\mathcal{P}^{(k)}_{\nu^{(k)}_{i,j}}$ and $\mathcal{P}^{(\ell)}_{\nu^{(\ell)}_{i,j}}$, from the two different partitions, $\mathcal{P}^{(k)}$ and $\mathcal{P}^{(\ell)}$ respectively, which intersect at both (i,j) and (n,m), which contradicts the 1-overlap property. We can therefore conclude that two partitions $\mathcal{P}^{(k)}$ and $\mathcal{P}^{(\ell)}$ that share the 1-overlap property with each other and the Cartesian partitions correspond to mutually orthogonal Latin squares. □

C. SIC-compatibility for mutually unbiased POVMs

We now turn to the problem of determining conditions under which a given set of mutually unbiased POVMs can be marginals of a common SIC. Recall that any marginal POVM E^k is specified by a partition $\mathcal{P}^{(k)}$ of G such that each positive operator $\mathsf{E}^k(\nu)$ is the sum of the SIC elements from one of the bins:

$$\mathsf{E}^k(\nu) = \sum_{\mathsf{G}(i) \in \mathcal{P}^{(k)}_\nu} \mathsf{G}(i).$$

Proposition 3. *If a collection of at least three mutually unbiased POVMs E^k are given as marginals of a SIC then the partition associated with each E^k is a d-partition $\mathcal{P}^{(k)}$. Moreover, d-partitions associated with different marginals E^k and E^ℓ satisfy the 1-overlap property.*

Proof. We begin with a collection of mutually unbiased POVMs E^k which do not have a fixed number of elements, and each $\mathsf{E}^k(\nu)$ is composed of an unspecified number of elements from the SIC. We show first that in order to satisfy the mutual unbiasedness condition $\mathrm{tr}\big[\mathsf{E}^k(\nu)\mathsf{E}^\ell(\mu)\big] = 1/d$, each of the E^k_ν must be composed of d SIC elements; from this we deduce the 1-overlap property.

Consider two partitions $\mathcal{P}^{(k)}$ and $\mathcal{P}^{(\ell)}$ containing m_k and m_ℓ bins, respectively. We do not make any restrictions on the number of elements from the SIC that are in any of the bins in $\mathcal{P}^{(k)}$ and $\mathcal{P}^{(\ell)}$, and so we denote $\big|\mathcal{P}^{(k)}_\nu\big| = n^{(k)}_\nu$, and likewise $\big|\mathcal{P}^{(\ell)}_\mu\big| = n^{(\ell)}_\mu$, where $\sum_\nu n^{(k)}_\nu = \sum_\mu n^{(\ell)}_\mu = d^2$. We denote $\big|\mathcal{P}^{(k)}_\nu \cap \mathcal{P}^{(\ell)}_\mu\big| = a^{k,\ell}_{\nu,\mu}$, that is $a^{k,\ell}_{\nu,\mu}$ is the number of elements that overlap between $\mathcal{P}^{(k)}_\nu$ and $\mathcal{P}^{(\ell)}_\mu$. These numbers must satisfy $\sum_\nu a^{k,\ell}_{\nu,\mu} = n^{(\ell)}_\mu$ and $\sum_\mu a^{k,\ell}_{\nu,\mu} = n^{(k)}_\nu$ because every element in $\mathcal{P}^{(\ell)}_\mu$ must appear in exactly one of the bins in $\mathcal{P}^{(k)}$, and likewise for $\mathcal{P}^{(k)}_\nu$. With this notation we obtain

$$\begin{aligned}\frac{1}{d} &= \mathrm{tr}\left[\mathsf{E}^k(\nu)\mathsf{E}^\ell(\mu)\right] \\ &= \frac{1}{d^2}a^{k,\ell}_{\nu,\mu} + \frac{1}{d^2(d+1)}(n^{(k)}_\nu n^{(\ell)}_\mu - a^{k,\ell}_{\nu,\mu}) \\ &= \frac{1}{d^2(d+1)}\left(d a^{k,\ell}_{\nu,\mu} + n^{(k)}_\nu n^{(\ell)}_\mu\right).\end{aligned} \tag{23}$$

Summing over μ we obtain

$$\sum_\mu \frac{1}{d} = \frac{m_\ell}{d} = \frac{1}{d^2(d+1)}\left(d n^{(k)}_\nu + d^2 n^{(k)}_\nu\right) = \frac{1}{d} n^{(k)}_\nu,$$

hence, $m_\ell = n^{(k)}_\nu$, and likewise by summing over ν we find that $m_k = n^{(\ell)}_\mu$. This means that all bins of $\mathcal{P}^{(k)}$ have the same number of elements, m_ℓ, the number of bins in $\mathcal{P}^{(\ell)}$, and likewise all bins in $\mathcal{P}^{(\ell)}$ have the same number of elements, m_k, the number of bins in $\mathcal{P}^{(k)}$. We

may thus drop the ν and μ subscripts from $n_\nu^{(k)}$ and $n_\mu^{(\ell)}$, respectively, and simply consider $n^{(k)}$ and $n^{(\ell)}$. With this new notation we have $n^{(k)}m_k = n^{(\ell)}m_\ell = m_k m_\ell = d^2$.

We now consider three marginals: $\mathrm{tr}\big[\mathsf{E}^k(\nu)\mathsf{E}^j(\sigma)\big] = \mathrm{tr}\big[\mathsf{E}^\ell(\mu)\mathsf{E}^j(\sigma)\big] = 1/d$ for all ν, μ, σ. By repeating the preceding argument we find that $n^{(k)} = n^{(\ell)} = m_j$, and so the bins in partitions $\mathcal{P}^{(k)}$ and $\mathcal{P}^{(\ell)}$ contain the same numbers of elements; this also shows us that $m_k = m_\ell$, and so $d^2 = m_k m_\ell = m_k^2$, hence $m_k = n^{(k)} = d$, and likewise for the other partitions.

We can now return to equation (23):

$$\frac{1}{d} = \frac{1}{d^2(d+1)}(da_{\nu,\mu}^{k,\ell} + n^{(k)}n^{(\ell)}) = \frac{1}{d^2(d+1)}(da_{\nu,\mu}^{k,\ell} + d^2).$$

We conclude that $a_{\nu,\mu}^{k,\ell} = 1$. Since the choice of bins was arbitrary, this result holds in general. □

Corollary 1. *For every SIC in $\mathcal{H}_d$ there exist sets of at least three and at most $d+1$ marginals that are mutually unbiased POVMs. For $d = 6$ there are no more than three marginal POVMs that are mutually unbiased.*

The first statement is a direct consequence of Lemma 2 and Theorem 1. The latter statement follows from the fact that there are no pairs of mutually orthogonal Latin squares of order 6 [22], so that the 1-overlap property required by Proposition 3 cannot be satisfied for more than three partitions.

D. Commutative case

We are interested in constructing three or more mutually unbiased POVMs E^k that arise as marginals from a SIC G. We have seen so far that it is necessary to define such marginals via d-partitions of G that satisfy the 1-overlap property. Thus the mutually unbiased POVMs E^k will satisfy conditions (19)-(22). If one could show that such mutually unbiased POVMs can be constructed so that each POVM E^k is commutative, that is the elements $\mathsf{E}^k(\nu)$ are mutually commuting for fixed k, then there is a possibility to extract a system of MUBs from these mutually unbiased POVMs.

In this commutative case, the elements $\mathsf{E}^k(\nu)$ of each E^k share an orthonormal eigenbasis and so have a decomposition in terms of the projections $\mathsf{P}^k(i)$ onto the elements of the eigenbasis:

$$\mathsf{E}^k(\nu) = \sum_{i=1}^{d} \lambda_{\nu,i}^k \mathsf{P}^k(i), \tag{24}$$

where the $\lambda_{\nu,i}^k$ are the eigenvalues of $\mathsf{E}^k(\nu)$ satisfying $\mathsf{E}^k(\nu)\mathsf{P}^k(i) = \lambda_{\nu,i}^k \mathsf{P}^k(i)$. Equation (24) shows that the commutative POVM E^k is a smearing of the PVM $\mathsf{P}^k := \{\mathsf{P}^k(i)\}_{i=1}^d$.

By making use of equation (24), and the orthogonality of the $\mathsf{P}^k(i)$, we can find some requirements the eigenvalues $\big(\lambda_{\nu,i}^k\big)$ must satisfy.

Firstly, we consider the trace-one property (19) and the normalisation $\sum_\nu \mathsf{E}^k(\nu) = I$.

$$\begin{aligned} 1 &= \mathrm{tr}\left[\mathsf{E}^k(\nu)\right] = \sum_i \lambda_{\nu,i}^k \mathrm{tr}\big[\mathsf{P}^k(i)\big] \\ &= \sum_i \lambda_{\nu,i}^k = \boldsymbol{\lambda}_\nu^k \cdot \mathbb{I}; \end{aligned} \tag{25a}$$

$$\begin{aligned} I &= \sum_\nu \mathsf{E}^k(\nu) = \sum_\nu \sum_i \lambda_{\nu,i}^k \mathsf{P}^k(i) = \sum_i \sum_\nu \lambda_{\nu,i}^k \mathsf{P}^k(i), \\ &\text{so } \sum_\nu \lambda_{\nu,i}^k = 1, \quad \text{or, equivalently} \quad \sum_\nu \boldsymbol{\lambda}_\nu^k = \mathbb{I}. \end{aligned} \tag{25b}$$

where $\boldsymbol{\lambda}_\nu^k = (\lambda_{\nu,1}^k, \ldots, \lambda_{\nu,d}^k)$ is the vector of eigenvalues of $\mathsf{E}^k(\nu)$, $\mathbb{I} = (1, \ldots, 1)$ in equation (25a), and in equation (25b) we have made use of the linear independence of the $\mathsf{P}^k(i)$. If we form a matrix, $\Lambda^k = \big(\lambda_{\nu,i}^k\big)$, of eigenvalues for the elements of the k-th mutually unbiased POVM, then equations (25a), (25b) are seen to entail that Λ^k is a doubly stochastic matrix.

If we examine equations (20) and (21) using equation (24) we find that

$$\frac{2}{d+1} = \mathrm{tr}\left[\big(\mathsf{E}^k(\nu)\big)^2\right] = \sum_i \big(\lambda_{\nu,i}^k\big)^2 = \left|\boldsymbol{\lambda}_\nu^k\right|^2, \tag{26a}$$

$$\frac{1}{d+1} = \mathrm{tr}\left[\mathsf{E}^k(\nu)\mathsf{E}^k(\mu)\right] = \sum_i \lambda_{\nu,i}^k \lambda_{\mu,i}^k = \boldsymbol{\lambda}_\nu^k \cdot \boldsymbol{\lambda}_\mu^k. \tag{26b}$$

Note that, in line with Remark 1, the unit trace property (25a) is an immediate consequence of the (self-)overlap conditions (26a), (26b) together with the normalisation condition $\sum_\nu \mathsf{E}^k(\nu) = I$. Alternatively, the self-overlap property (26a) follows from the mutual overlap property (26b) and the unit trace and normalisation conditions.

Making use of equations (25a) and (26a) one can see that the endpoints of the eigenvalue vectors $\boldsymbol{\lambda}_\nu^k$ lie on the intersection between the $d-1$-dimensional hyperplane $\boldsymbol{\lambda}_\nu^k \cdot \mathbb{I} = 1$ and the $d-1$-sphere centred at the origin with radius $[2/(d+1)]^{1/2}$. Since the $\boldsymbol{\lambda}_\nu^k$ have equal lengths and overlaps, their endpoints span the vertices of a regular simplex with centre $\frac{1}{d}\mathbb{I}$ in that hyperplane. This can be confirmed by considering the vectors

$$\boldsymbol{r}_\nu = \boldsymbol{\lambda}_\nu^k - \tfrac{1}{d}\mathbb{I}, \tag{27}$$

These vectors connect the centre of the simplex with its vertices and they have constant lengths and overlaps:

$$\begin{aligned} |\boldsymbol{r}_\nu|^2 &= \left|\boldsymbol{\lambda}_\nu^k\right|^2 + |(1/d)\mathbb{I}|^2 - (2/d)\boldsymbol{\lambda}_\nu^k \cdot \mathbb{I} \\ &= \frac{2}{d+1} - \frac{1}{d} = \frac{d-1}{d(d+1)}, \end{aligned} \tag{28a}$$

$$\begin{aligned} \boldsymbol{r}_\nu \cdot \boldsymbol{r}_\mu &= \boldsymbol{\lambda}_\nu^k \cdot \boldsymbol{\lambda}_\mu^k + |(1/d)\mathbb{I}|^2 - (1/d)(\boldsymbol{\lambda}_\nu^k + \boldsymbol{\lambda}_\mu^k) \cdot \mathbb{I} \\ &= \frac{1}{d+1} - \frac{1}{d} = -\frac{1}{d(d+1)}. \end{aligned} \tag{28b}$$

Equation (28b) can be rewritten as

$$\boldsymbol{r}_\nu \cdot \boldsymbol{r}_\mu = |\boldsymbol{r}_\nu|\,|\boldsymbol{r}_\mu| \cos\theta = \frac{d-1}{d(d+1)} \cos\theta = -\frac{1}{d(d+1)}$$
$$\Rightarrow \cos\theta = -\frac{1}{d-1},$$

where the constancy of the angle θ between $\boldsymbol{r}_\nu$ and $\boldsymbol{r}_\mu$ reflects the regularity of the simplex. We summarize:

Proposition 4. *Let E^k be a commutative POVM whose elements $\mathsf{E}^k(\nu) = \sum_i \lambda^k_{\nu,i} \mathsf{P}^k(i)$ have unit trace (hence the eigenvalue matrix Λ^k is doubly stochastic) and satisfy the overlap condition* (26b)*. Then the d eigenvalue vectors $\boldsymbol{\lambda}^k_\nu \in \mathbb{R}^d$ point to the vertices of a regular $d-1$-simplex lying on the intersection of the $d-1$-dimensional hyperplane $\boldsymbol{\lambda}^k_\nu \cdot \mathbb{I} = 1$ and the $d-1$-sphere of radius $(2/(d+1))^{1/2}$ centred at the origin.*

Proposition 4 provides a geometric interpretation of properties that a set of d positive operators with the same eigenbasis must satisfy in order to arise as a commutative marginal of a SIC associated with a d-partition. These properties are also used in proving the following theorem.

Theorem 2. *Let E^k and E^ℓ be two commutative POVMs whose elements have unit trace and satisfy the overlap property* (26b)*. If their decompositions in terms of eigenprojections are given as in equation* (24)*, i.e.*

$$\mathsf{E}^k(\nu) = \sum_i \lambda^k_{\nu,i} \mathsf{P}^k(i), \quad \mathsf{E}^\ell(\mu) = \sum_j \lambda^\ell_{\mu,j} \mathsf{P}^\ell(j), \tag{29}$$

then the following equivalence holds:

$$\operatorname{tr}\left[\mathsf{E}^k(\nu)\mathsf{E}^\ell(\mu)\right] = \frac{1}{d} \;\forall\, \mu,\nu$$
$$\iff \operatorname{tr}\left[\mathsf{P}^k(i)\mathsf{P}^\ell(j)\right] = \frac{1}{d} \;\forall\, i,j\,.$$

Proof. Given equation (29), we verify that the condition $\operatorname{tr}\left[\mathsf{P}^k(i)\mathsf{P}^\ell(j)\right] = 1/d$ for all i,j leads directly to $\operatorname{tr}\left[\mathsf{E}^k(\nu)\mathsf{E}^\ell(\mu)\right] = 1/d$ for all ν,μ. Since

$$\operatorname{tr}\left[\mathsf{E}^n(\mu)\right] = \sum_{i=1}^d \lambda^n_{\mu,i} \operatorname{tr}\left[\mathsf{P}^n(i)\right] = \sum_{i=1}^d \lambda^n_{\mu,i} = 1, \quad n = k,\ell, \tag{30}$$

we have that

$$\operatorname{tr}\left[\mathsf{E}^k(\mu)\mathsf{E}^\ell(\nu)\right] = \sum_{i=1}^d \lambda^k_{\mu,i} \sum_{j=1}^d \lambda^\ell_{\nu,j} \operatorname{tr}\left[\mathsf{P}^k(i)\mathsf{P}^\ell(j)\right]$$
$$= \left(\sum_{i=1}^d \lambda^k_{\mu,i}\right)\left(\sum_{j=1}^d \lambda^\ell_{\nu,j}\right)\frac{1}{d} = \frac{1}{d}, \tag{31}$$

whenever $k \neq \ell$, and so the smeared operators are mutually unbiased. (Note that this implication does not rely on the overlap property (26b).)

Next, we prove the converse implication. By making use of equation (29), we see that

$$\operatorname{tr}\left[\mathsf{E}^k(\nu)\mathsf{E}^\ell(\mu)\right] = \frac{1}{d} = \sum_{i,j} \lambda^k_{\nu,i}\, \lambda^\ell_{\mu,j} \operatorname{tr}\left[\mathsf{P}^k(i)\mathsf{P}^\ell(j)\right]$$
$$=: \sum_{i,j} \lambda^k_{\nu,i}\, q^{k\ell}_{ij}\, \lambda^\ell_{\mu,j}, \tag{32}$$

or equivalently,

$$\Lambda^k Q^{k\ell} (\Lambda^\ell)^T = \frac{1}{d} U, \tag{33}$$

where $Q^{k\ell} = \left(q^{k\ell}_{ij}\right) = \left(\operatorname{tr}\left[\mathsf{P}^k(i)\mathsf{P}^\ell(j)\right]\right)$ and $U_{ij} = 1\ \forall\ i,j$. Because the rows of Λ^k (and likewise for Λ^ℓ) correspond to the vertices of a regular simplex, they are linearly independent, and this means that Λ^k (and Λ^ℓ respectively) is invertible. Therefore, there exist two matrices, Γ^k and Γ^ℓ, such that

$$\Gamma^k \Lambda^k = \Gamma^\ell \Lambda^\ell = I,$$

and so

$$Q^{k\ell} = \frac{1}{d}\, \Gamma^k U (\Gamma^\ell)^T.$$

Note that, thanks to the (row) stochasticity of Λ^k and Λ^ℓ, the matrices Γ^k and $(\Gamma^\ell)^T$ are such that the sum of each row in the first case and the sum of each column in the second case is one. Indeed, a matrix A is such that the sum of each row is one if and only if $A\,\mathbb{I}^T = \mathbb{I}^T$ where, $\mathbb{I} = (1,1,\ldots,1)$. Thanks to the row stochasticity of Λ^k, we have $\mathbb{I}^T = I\,\mathbb{I}^T = (\Gamma^k\Lambda^k)\,\mathbb{I}^T = \Gamma^k(\Lambda^k\,\mathbb{I}^T) = \Gamma^k\,\mathbb{I}^T$ which proves that the sum of each row in Γ^k is 1. The same reasoning shows that the sum of each row in Γ^ℓ is 1 which implies that the sum of each column in $(\Gamma^\ell)^T$ is 1. We note that, in general, Γ^k and Γ^ℓ are not stochastic since they are not positive definite. It follows that

$$\Gamma^k U = U; \qquad U(\Gamma^\ell)^T = U$$

and

$$Q^{k\ell} = \frac{1}{d}\,\Gamma^k U (\Gamma^\ell)^T = \frac{1}{d}\,U,$$

which completes the proof. □

We summarize the implications of the results from this section, using the fact that the conditions of Theorem 2 are satisfied for mutually unbiased POVMs that are marginals of a SIC.

Corollary 2. *Let G be a SIC which possesses a family of commutative marginals E^k generated by d-partitions that share the 1-overlap property (hence they are mutually unbiased). Then the orthonormal eigenbases shared by elements of the same marginal are mutually unbiased.*

It is an open question whether every SIC possesses commutative marginals arising from a d-partition.

IV. FROM MUBS TO SICS

We consider next the problem of constructing a SIC from a given collection of MUBs. As a preliminary investigation we establish necessary conditions for a family of mutually unbiased POVMs to arise as marginals of a SIC. In the case where there are $d+1$ mutually unbiased POVMs satisfying certain properties to be specified below, it is possible to establish a formula for the corresponding SIC elements. This requires us to invert the system of equations (18),

$$\mathsf{E}^k(\nu) = \sum_{\mathsf{G}(i)\in\mathcal{P}_\nu^{(k)}} \mathsf{G}(i) \quad (\nu = 1,\dots,d,\ k = 1,\dots,d+1),$$

bearing in mind that the underlying d-partitions satisfy the 1-overlap property. We can take guidance from the construction shown in the qubit case. We begin with some important combinatorial observations.

A. Combinatorial interlude

We consider an $(d+1)\times d$ array of points with a system of paths with the property that every path is of length $d+1$ containing one element from each row and any two paths share the *1-overlap property*, that is, they intersect in exactly one point.

Lemma 3. *Let $\mathcal{E}$ be a $(d+1)\times d$ array of points. There are at most d^2 paths p_i through $\mathcal{E}$ containing exactly one point from each row such that any two paths intersect with each other exactly once.*

Proof. Consider all paths that start, and therefore intersect, on the j^{th} element in the first row, i.e., at $\mathcal{E}_{1j}$; from this point on no two of these paths may intersect at any further point. Since no point within the second row can appear within two paths beginning at $\mathcal{E}_{1j}$, we can have at most d possible paths passing through the second row. Given that we have d elements within the first row, we can therefore have at most d^2 paths with the required properties. □

There is a fundamental connection between the array $\mathcal{E}$ with its path system described above and the $d\times d$ array used to define d-partitions of a SIC with the 1-overlap property.

Proposition 5. *A $d\times d$ array A with a complete set of $d+1$ partitions satisfying the 1-overlap property between bins, each of order d, of different d-partitions is equivalent to a $(d+1)\times d$ array B with a complete set of d^2 downwards paths of length $d+1$ that satisfy the 1-overlap property between any pair of paths; the equivalence consists in the correspondence of the points and paths in A with the paths and points in B, respectively.*

Proof. We will start with the $d\times d$ array $A=\{a_{i,j}\}$, which has partitions satisfying the 1-overlap property between bins/paths $\mathcal{P}_\nu^{(k)}$, $\mathcal{P}_\mu^{(l)}$, of different partitions $\mathcal{P}^{(k)}$, $\mathcal{P}^{(l)}$ of A. As noted in Section III B, $\left|\mathcal{P}_\nu^{(k)}\cap\mathcal{P}_\mu^{(\ell)}\right| = 1$ when $k\neq\ell$ and, by Lemma 2, there exist at most $d+1$ partitions. We assume that A possesses $d+1$ partitions with the 1-overlap property. We can construct a $(d+1)\times d$ array B as follows: each point of B corresponds to a bin/path, and the d bins from a given partition are arranged in rows. For example, B could be the array $\{b_{k,\nu}\}=\{\mathcal{P}_\nu^{(k)}\}$.

Now, for each point $a_{i,j}$ in A we can define a path $p_{i,j}$ on B as follows: $p_{i,j}=\{\mathcal{P}^{(1)}_{r_1(i,j)},\dots,\mathcal{P}^{(d+1)}_{r_{d+1}(i,j)}\}$ where, $a_{i,j}\in\mathcal{P}^{(k)}_{r_k(i,j)}$, $k=1,\dots,d+1$. The paths on B are strictly downwards and this corresponds to the fact that each point in A appears only once in a given partition.

Note that each path $p_{i,j}$ on B contains $d+1$ bins $\mathcal{P}^{(l)}_{r_l(i,j)}$, $l=1,\dots,d+1$, each bin $\mathcal{P}^{(l)}_{r_l(i,j)}$ contains the point $a_{i,j}$ plus $d-1$ points of A, and, by the 1-overlap property between the bins $\mathcal{P}^{(l)}_{r_l(i,j)}$, the point $a_{i,j}$ is the only one they have in common. Therefore a total of $(d+1)(d-1)+1=d^2$ distinct points (all the points in A) are involved in each path on B. This means that for any point $a_{i,j}$ and for any path $p_{\nu,\mu}=\{\mathcal{P}^{(1)}_{r_1(\nu,\mu)},\dots,\mathcal{P}^{(d+1)}_{r_{d+1}(\nu,\mu)}\}$, there is an index k such that $a_{i,j}\in\mathcal{P}^{(k)}_{r_k(\nu,\mu)}$. Therefore, two arbitrary paths $p_{\nu,\mu}$, $p_{i,j}$ on B must overlap at least once. Indeed, $a_{i,j}\in\mathcal{P}^{(l)}_{r_l(i,j)}$, for all l, and, by the previous reasoning, there is a k such that $a_{i,j}\in\mathcal{P}^{(k)}_{r_k(\nu,\mu)}$. That implies $\mathcal{P}^{(k)}_{r_k(i,j)}\cap\mathcal{P}^{(k)}_{r_k(\nu,\mu)}\neq\emptyset$ and then $\mathcal{P}^{(k)}_{r_k(\nu,\mu)}=\mathcal{P}^{(k)}_{r_k(i,j)}$ since $\mathcal{P}^{(k)}_{r_k(\nu,\mu)}$ and $\mathcal{P}^{(k)}_{r_k(i,j)}$ belong to the same partition of A and can have a common point only if they coincides.

The 1-overlap property defined on A means also that the two paths $p_{\nu,\mu}$, $p_{i,j}$ overlap exactly once: if they overlap more than once then, there are two indices, k,l, such that $\mathcal{P}^{(k)}_{r_k(\nu,\mu)}=\mathcal{P}^{(k)}_{r_k(i,j)}$ and $\mathcal{P}^{(l)}_{r_l(\nu,\mu)}=\mathcal{P}^{(l)}_{r_l(i,j)}$ and then, there exist two bins, $\mathcal{P}^{(k)}_{r_k(\nu,\mu)}$, $\mathcal{P}^{(l)}_{r_l(\nu,\mu)}$, from different partitions of A such that $a_{\nu,\mu},a_{i,j}\in\mathcal{P}^{(k)}_{r_k(\nu,\mu)}$ and $a_{\nu,\mu},a_{i,j}\in\mathcal{P}^{(l)}_{r_l(\nu,\mu)}$. This violates the 1-overlap property defined on A. Thus we have proved that the 1-overlap property between bins in different partitions of A implies the 1-overlap property between any pair of paths on B.

Conversely, let a $(d+1)\times d$ array B be given with the path system as described. The 1-overlap property defined on B entails that, by Lemma 3, we have at most d^2 strictly downward paths where d paths intersect on any given point. Here we assume that that number is d^2. We define a $d\times d$ array $A=\{a_{\nu,\mu}\}$ where, $a_{\nu,\mu}:=p^\mu_\nu$ is the μ^{th} path on B containing the point $b_{1,\nu}$. With this construction and using the 1-overlap property on B, we define the paths on A to correspond to the points in B as follows: to a point $b_{i,j}$, $i\neq 1$, in B there corresponds the path on A, $\{p_1^{\mu_1(i,j)},\dots,p_d^{\mu_d(i,j)}\}$, such that $b_{i,j}\in$

$p_k^{\mu_k(i,j)}$ for each $k = 1, \ldots, d$, while to a point $b_{1,j}$ there corresponds the path $\{p_j^1, \ldots, p_j^d\}$.

Since the paths on B are strictly downward, each row of B forms a partition of its paths. Therefore, if we take d paths on A, each corresponding to a point in a particular row of B, we get a d-partition of the points in A. That is clearly true for the families of paths corresponding to the points $b_{1,j}$, $j = 1, \ldots, d$, which define the partition of A in horizontal bins. It is also true for the family of paths $\{(p_1^{\mu_1(i,k)}, \ldots, p_d^{\mu_d(i,k)})\}$, $k = 1, \ldots, d$, corresponding to the row $(b_{i,k})$, $i \neq 1$, $k = 1, \ldots, d$, which cannot overlap. Indeed, if it were $p_j^{\mu_j(i,k)} = p_j^{\mu_j(i,l)}$, we would have $b_{i,k}, b_{i,l} \in p_j^{\mu_j(i,k)}$ which means that the path $p_j^{\mu_j(i,k)}$ is not downward. In other words, a set of d non-intersecting paths on A, which correspond to a row on B, form a partition of the points on A.

As a consequence of the 1-overlap property on the paths on B, any two paths on B intersect at only one point, which on A corresponds to the property that any two paths from different partitions intersect only once: two paths on A intersecting more than once correspond to two points on B which are coincident with the same two paths twice, which cannot occur because of the 1-overlap property. For example, if the paths $(p_1^{\mu_1(i,j)}, \ldots, p_d^{\mu_d(i,j)})$, and $(p_1^{\mu_1(\nu,\mu)}, \ldots, p_d^{\mu_d(\nu,\mu)})$ corresponding to the points $b_{i,j}$ and $b_{\nu,\mu}$, $i, \nu \neq 1$, respectively, overlap twice then, there are two indices l, s, such that $p_l^{\mu_l(i,j)} = p_l^{\mu_l(\nu,\mu)}$ and $p_s^{\mu_s(i,j)} = p_s^{\mu_s(\nu,\mu)}$. That implies $b_{i,j}, b_{\nu,\mu} \in p_l^{\mu_l(i,j)}$ as well as $b_{i,j}, b_{\nu,\mu} \in p_s^{\mu_s(i,j)}$ which contradicts the 1-overlap property of the paths on B. The same reasoning applies if one of the two paths is replaced by an horizontal path on A. So by starting with B and its path system, we have managed to construct A with its own path system satisfying the required properties. □

B. Construction of SIC elements from mutually unbiased POVMs

We assume that a collection of $d+1$ POVMs E^k is given, each with d outcomes, and introduce a $(d+1) \times d$ array $\mathcal{E}$ with points $\mathcal{E}_{k\nu} = \mathsf{E}^k(\nu)$:

$$\mathcal{E} = \begin{matrix} \mathsf{E}^1(1) & \ldots & \mathsf{E}^1(d) \\ \vdots & \ddots & \vdots \\ \mathsf{E}^{d+1}(1) & \ldots & \mathsf{E}^{d+1}(d) \end{matrix} . \tag{34}$$

Let us now assume that these POVMs E^k are marginals of a d^2-outcome observable $\mathsf{G} = \{\mathsf{G}(i)\}_{i=0}^{d^2-1}$; moreover, we assume that each marginal is associated with a d-partition, where any two partitions satisfy the 1-overlap property. This entails that no two elements belonging to the same POVM have an operator $\mathsf{G}(i)$ in common, whilst two elements from different POVMs must share just one. In this case, each $\mathsf{G}(i)$ belongs to one element

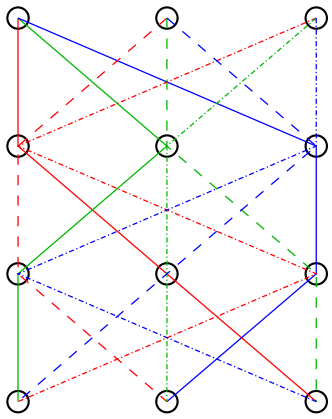

FIG. 2. d^2 Paths with the 1-overlap property for $d = 3$.

from each of the $d+1$ POVMs. On the array $\mathcal{E}$, these relations correspond to paths $\mathcal{P}_i$, defined as subsets of those elements that share $\mathsf{G}(i)$. From the above constraints on the d^2 positive operators two properties of these paths are as follows:

1. Given that no $\mathsf{G}(i)$ can occur within two elements of the same POVM E^k, the paths must be strictly downwards, i.e. they cannot contain any horizontal routes through the array;

2. Because any two elements from different E^k and E^ℓ share a single operator $\mathsf{G}(i)$, any two paths through $\mathcal{E}$ must intersect at a single point: if two paths were to intersect twice, then the points where the intersections occurred would correspond to two elements that have two operators, $\mathsf{G}(i)$ and $\mathsf{G}(j)$ say, in common, thereby violating the construction requirements.

By virtue of Proposition 5, it is ensured that there are d^2 downward paths of length $d+1$ in $\mathcal{E}$ such that any two paths share the 1-overlap property. An example of this construction is given in Fig. 2.

We now consider the path $\mathcal{P}_i$ connecting all points in the array $\mathcal{E}$ of marginal POVM elements defined in (34) which contain $\mathsf{G}(i)$. At this point we define the operators

$$E_i = \sum_k \mathsf{E}^k\big(\nu(i,k)\big), \tag{35}$$

where $\mathsf{E}^k\big(\nu(i,k)\big)$ is the element in the k-th POVM E^k incident with the path $\mathcal{P}_i$. Note that E_i is the sum of $d+1$ operators, all sharing just $\mathsf{G}(i)$ and so all other operators $\mathsf{G}(j)$ included within the path can occur at most once. Each of the $d+1$ operators $\mathsf{E}^k\big(\nu(i,k)\big)$ is the sum of d SIC elements, one of which is $\mathsf{G}(i)$, and the remaining $d-1$ elements $\mathsf{G}(j)$ must be unique to $\mathsf{E}^k\big(\nu(i,k)\big)$. Hence

a total of $(d+1)(d-1) = d^2-1$ elements of G other than $\mathsf{G}(i)$ are required. Their sum is equal to $I - \mathsf{G}(i)$ since $\sum_{j=0}^{d^2-1} \mathsf{G}(j) = I$. Therefore,

$$\begin{aligned} E_i &= \sum_k \mathsf{E}^k\big(\nu(i,k)\big) = (d+1)\mathsf{G}(i) + (I - \mathsf{G}(i)) \\ &= d\mathsf{G}(i) + I. \end{aligned}$$

Hence we obtain the following.

Proposition 6. *Assume a d^2-outcome POVM G has $d+1$ marginals E^k associated with a complete system of $d-$partitions satisfying the 1-overlap property. Then the elements $\mathsf{G}(k)$ can be recovered from the E^k via*

$$\mathsf{G}(k) = \frac{1}{d}(E_k - I) \tag{36}$$

where the operators E_k are defined in equation (35).

We are now ready to prove the main result of this section.

Theorem 3. *Consider a family of $d+1$ POVMs E^k which are mutually unbiased, i.e.,*

$$\operatorname{tr}\big[\mathsf{E}^k(\mu)\mathsf{E}^\ell(\nu)\big] = \frac{1}{d},\ k,\ell = 1,\dots,d+1,\ \nu,\mu = 1,\dots d,$$

and assume that the elements also satisfy

$$\operatorname{tr}\big[\mathsf{E}^k(\mu)\mathsf{E}^k(\nu)\big] = \frac{1}{d+1},\ k = 1,\dots,d+1,\ \nu \neq \mu.$$

Further assume that there are d^2 sets $\mathcal{P}_i$, $i = 0,1,\dots,d^2-1$, consisting of $d+1$ elements, one chosen from each of the E^k, such that the 1-overlap property is fulfilled. Let operator E_i be the sum of the elements in $\mathcal{P}_i$. Then the d^2 operators $\mathsf{G}(i) := \frac{1}{d}(E_i - I)$ form a SIC if and only if they are positive.

Proof. We will be using the observation made in Remark 1, which entails that under the conditions of the theorem the POVMs also satisfy

$$\operatorname{tr}\big[\mathsf{E}^k(\mu)\big] = 1, \quad \operatorname{tr}\big[\mathsf{E}^k(\mu)^2\big] = \frac{2}{d+1}.$$

We verify the SIC conditions (3)-(4). First,

$$\operatorname{tr}[\mathsf{G}(i)] = \frac{1}{d}\operatorname{tr}[E_i - I] = \frac{1}{d}(d+1) - 1 = \frac{1}{d}, \tag{37}$$

where we have used $\operatorname{tr}\big[E_i\big] = \sum_k \operatorname{tr}\big[\mathsf{E}^k\big(\nu(i,k)\big)\big] = d+1$. Secondly,

$$\operatorname{tr}\big[\mathsf{G}(i)^2\big] = \frac{1}{d^2}\operatorname{tr}\big[E_i^2 - 2E_i + I\big] = \frac{1}{d^2}(\operatorname{tr}\big[E_i^2\big] - d - 2),$$

Note that $\operatorname{tr}\big[E_i^2\big] = \operatorname{tr}\Big[\big(\sum_k \mathsf{E}^k\big(\nu(i,k)\big)\big)^2\Big]$ contains $d+1$ terms of the form $\operatorname{tr}\Big[\big(\mathsf{E}^k(\nu)\big)^2\Big] = 2/(d+1)$ and $d(d+1)$ terms of the form $\operatorname{tr}\big[\mathsf{E}^k(\mu)\mathsf{E}^\ell(\nu)\big] = 1/d$ since any two distinct elements in a given E_i must belong to different POVM. Therefore,

$$\operatorname{tr}\big[(E_i)^2\big] = 2(d+1)/(d+1) + d(d+1)/d = d+3,$$

and so

$$\operatorname{tr}\big[\mathsf{G}(i)^2\big] = \frac{1}{d^2}(\operatorname{tr}\big[E_i^2\big] - d - 2) = \frac{1}{d^2}. \tag{38}$$

This coincides with the required value for this quantity.

We are ready to determine the trace of $\mathsf{G}(i)\mathsf{G}(j)$ for $i \neq j$:

$$\begin{aligned} \operatorname{tr}[\mathsf{G}(i)\mathsf{G}(j)] &= \frac{1}{d^2}\operatorname{tr}[E_iE_j - E_i - E_j + I] \\ &= \frac{1}{d^2}(\operatorname{tr}[E_iE_j] - d - 2). \end{aligned} \tag{39}$$

The product E_iE_j consists of $(d+1)^2$ terms: $d+1$ will correspond to the product of two elements from the same POVM, i.e. $\mathsf{E}^k\big(\nu(i,k)\big)\mathsf{E}^k\big(\nu(j,k)\big)$, and $d(d+1)$ will be the product of elements from different POVMs, that is, $\mathsf{E}^k\big(\nu(i,k)\big)\mathsf{E}^\ell\big(\nu(j,\ell)\big)$. Because the intersection of $\mathcal{P}_i$ and $\mathcal{P}_j$ contains only one element, it follows that one of the $d+1$ terms $\mathsf{E}^k\big(\nu(i,k)\big)\mathsf{E}^k\big(\nu(j,k)\big)$ will have trace $2/(d+1)$, whilst the remaining d terms will have trace $1/(d+1)$, and the $d(d+1)$ terms of the form $\mathsf{E}^k\big(\nu(i,k)\big)\mathsf{E}^\ell\big(\nu(j,\ell)\big)$ will have trace $1/d$. Using these values we have that

$$\begin{aligned} \operatorname{tr}[E_iE_j] &= \frac{2}{d+1} + \frac{d}{d+1} + \frac{1}{d}(d(d+1)) \\ &= \frac{1}{d+1} + d + 2, \end{aligned}$$

and so equation (39) becomes

$$\operatorname{tr}[\mathsf{G}(i)\mathsf{G}(j)] = \frac{1}{d^2}(\operatorname{tr}[E_iE_j] - d - 2) = \frac{1}{d^2(d+1)}. \tag{40}$$

Finally we verify the normalisation condition:

$$\sum_{i=0}^{d^2-1} \mathsf{G}(i) = \frac{1}{d}\sum_{i=0}^{d^2-1} E_i - dI.$$

Each E_i contains $d+1$ POVM elements, each of which is from a different E^k. Each POVM element $\mathsf{E}^k(\mu)$ is shared by exactly d of the operators E_i, hence contributes d occurrences to $\sum_i E_i$. The sum of all $d(d+1)$ POVM elements is $(d+1)I$. This gives:

$$\sum_{i=0}^{d^2-1} \mathsf{G}(i) = \frac{1}{d}d(d+1)I - dI = I.$$

□

This theorem shows that the G has all the properties required of a SIC, except, possibly, the positivity of all $\mathsf{G}(i)$. In other words, G forms a SIC system and we can rephrase Theorem 3 as follows.

Corollary 3. *Under the assumptions of Theorem 3, the d^2 operators $\mathsf{G}(i)$ constructed from the mutually unbiased POVMs form a SIC system.*

Taking up the construction of commutative POVMs as smearings of mutually unbiased PVMs, we can complete the route from a family of $d+1$ MUBs to a SIC system.

Suppose a collection of MUBs $\{\varphi_i^k\}_{i=1}^d$ $(k = 1, \ldots, n)$ are given, so that $\mathsf{P}^k(i) = |\varphi_i^k\rangle\langle\varphi_i^k|$ are mutually unbiased PVMs. Applying a smearing of the form (24) with a stochastic matrix Λ^k to the PVMs P^k yields n POVMs E^k as in (24)

$$\mathsf{E}^k(\nu) = \sum_{i=1}^{d} \lambda_{\nu,i}^k \mathsf{P}^k(i),\ k = 1, \ldots, n,\ \nu = 1, \ldots, d$$

Proposition 7. *POVMs E^k, $k = 1, \ldots, n$ obtained as smearings of n mutually unbiased PVMs P^k via (??) are mutually unbiased if and only if all elements $\mathsf{E}^k(\nu)$ are unit trace operators (that is, the matrices Λ^k are doubly stochastic).*

Proof. The statement that the mutual unbiasedness of the POVMs E^k follows from the mutual unbiasedness of the corresponding PVMs together with unit trace property of the operators $\mathsf{E}^k(\mu)$ has already been shown in Theorem 2.

Conversely, assume that the operators $\mathsf{E}^k(\mu)$ and $\mathsf{E}^\ell(\nu)$ are mutually unbiased, that is, $\mathrm{tr}\big[\mathsf{E}^k(\mu)\mathsf{E}^\ell(\nu)\big] = \frac{1}{d}$ whenever $k \neq \ell$, then summing over ν and using the normalisation property $\sum_\nu \mathsf{E}^\ell(\nu) = I$ immediately gives $\mathrm{tr}\big[\mathsf{E}^k(\mu)\big] = 1$. □

Combining Theorem 3 and Proposition 7 we have obtained a construction of a SIC system from a complete family of MUBs.

V. COMPARISON WITH THE CONSTRUCTION OF WOOTTERS

Wootters [2] describes a geometric structure of dual systems of points and lines that turns out to be isomorphic to the two equivalent combinatorial structures composed of arrays and paths presented here. He begins by considering a set of d^2 points and, upon them, defines *mutually unbiased striations* as follows: a striation is a partitioning of the points into d *parallel lines* of d points each, that is, no point is contained in more than one line, and two striations are mutually unbiased if any two lines from different striations are coincident at a single point.

As we have argued before, in this language we are restricted to having at most $d+1$ mutually unbiased striations. Assuming that these d^2 points are placed into a $d \times d$ array, one begins by defining the horizontal and vertical striation in the logical way, and so any further mutually unbiased striation will correspond to a Latin square because, as in our construction, we cannot allow for any line to contain two points from the same row or column. Furthermore, any additional mutually unbiased striations will correspond to Latin squares that are orthogonal to the first Latin square, and each other, as is the case in our scheme. The difference lies in the association of points and lines: Wootters ascribes to each point α a selfadjoint operator A_α/d, and to each line λ a rank-1 projection $\mathsf{P}(\lambda)$, satisfying the following properties:

1. $\mathrm{tr}\,[A_\alpha/d] = 1/d$;
2. $\mathrm{tr}\,[(A_\alpha/d)(A_\beta/d)] = (1/d)\delta_{\alpha\beta}$;
3. $\sum_{\alpha\in\lambda} A_\alpha/d = \mathsf{P}(\lambda)$.

As a consequence of these conditions, a striation corresponds to a basis for a d-dimensional Hilbert space – we have d normalized rank-1 projections that are mutually orthogonal – and two mutually unbiased striations correspond to a pair of mutually unbiased bases.

However, as is pointed out in his paper, it is not clear how one constructs the operators A_α so that we may find these MUBs without in fact already having a complete set of MUBs to work backwards from. By contrast, our method provides us with the necessary operators corresponding to each point – the elements of a SIC POVM – and by going along a slightly more elongated path – by constructing striations corresponding to commutative mutually unbiased POVMs and then finding the joint eigenbasis for each mutually unbiased POVM – we are able in some cases to construct a set of MUBs (which will not always be complete).

Before considering the case for SIC POVMs, we note that the set of d^2 points and $d+1$ mutually unbiased striations to be considered correspond to an *affine plane of order d*. An affine plane of order d is a set of d^2 points and $d(d+1)$ lines satisfying the following conditions:

1. For any two points there exists exactly one line that is coincident with both;
2. for any point α and line λ not containing α, there exists a single line that is parallel (i.e. non-intersecting) with λ that is coincident with α;
3. there exist three points that are non-collinear.

It is known that affine planes exist if the order is a prime power. The situation for non-prime powers is not very well explored, although it is known that an affine plane of order 6 does not exist.

Following the discussion on MUBs, Wootters proceeds to consider the analogous geometric problem for constructing a SIC POVM. Again, this is considered in terms of lines passing through points in such a way that each line corresponds to a rank-1 projection $\mathsf{P}(i) = d\mathsf{G}(i)$, where $\mathsf{G}(i)$ is an element of our desired SIC POVM. In order to determine the number of points that lie on a given line, and indeed the total number of points to be consider, Wootters adopts an idea of Zauner [4] that provides a connection between the cardinality of a set of

points and the trace of its corresponding operator. If M is an operator, then let S_M denote the set of points corresponding to it within the given geometric construct (so in the previous paragraphs we would have that $S_{A_\alpha} = \{\alpha\}$, etc.). We now look for relations of the form

$$|S_M| = k \operatorname{tr}[M] \text{ and } |S_{M_1} \cap S_{M_2}| = k \operatorname{tr}[M_1 M_2] \quad (41)$$

for some constant k. Since the rank-1 projection $\mathsf{P}(\lambda)$ associated with the line λ must be trace one, it follows that the line contains k points within it. Furthermore, $\operatorname{tr}[\mathsf{P}(\lambda)\mathsf{P}(\mu)] = 1/(d+1)$ entails that distinct lines λ and μ intersect at $k/(d+1)$ points. This overlap must be an integer, hence k must be a multiple of $d+1$. For simplicity, one can choose $k = d+1$, and so any two lines intersect once. If one assumes that the operator associated with the entire set is the identity, and that each point lies on the same number of lines as any other point, then we have that there must exist $k \operatorname{tr}[I] = d(d+1)$ points and that each must lie on d lines. We note that the value of k was chosen for simplicity, whilst in our work, the value of k, i.e. the number of points each line must contain, is fixed.

Collecting all the information for the SIC POVM case, we see that one is considering $d(d+1)$ points and d^2 lines containing $d+1$ points each, where each point is contained in d lines and any two lines intersect at a single point. By performing a relabelling between the points and lines, we see that this construction yields an affine plane of order d. Note that this is similar to the situation for our construction, except that in our case the equivalence between the two systems of points and lines are in fact immediate, rather than the result of choosing a particular value of k, and that we are again reliant on the dimension being one that allows for an affine plane to be constructed.

Assuming that an affine plane can be constructed, Wootters identifies the task of finding a set of selfadjoint operators B_α associated with each point α such that the line i corresponds to their sum, which is equal to $\mathsf{P}(i) = d\mathsf{G}(i)$. In order to satisfy the necessary trace conditions, he requires that

1. $\operatorname{tr}\left[B_\alpha^2\right] = d/(d+1)^2$;
2. $\operatorname{tr}[B_\alpha B_\beta] = 1/d(d+1)^2$ if $\alpha \neq \beta$ and they share a line;
3. $\operatorname{tr}[B_\alpha B_\beta] = -1/(d+1)^2$ if $\alpha \neq \beta$ but they don't share a line.

However, as in the case for MUBs, it is not immediately obvious how these operators are constructed, without working backwards (and thereby defeating the purpose). Again, in our work we have the benefit that the operators associated with each point – elements of derived mutually unbiased POVMs – can be constructed readily.

VI. FROM COVARIANT SICS TO MUBS IN ODD PRIME POWER DIMENSIONS

After this comparison between our combinatorial scheme and Wootters' geometric scheme, we are now free to use geometric language, which is natural here. In particular, this section is devoted to developing a concrete example of the previous general setting. Given a finite covariant phase space observable acting on a Hilbert space of prime power dimension $d = p^n$ ($p \neq 2$), we construct $d+1$ marginals that are mutually unbiased POVMs. These marginals turn out to be smearings of $d+1$ MUBs, and hence are commutative (compare with the discussion at the end of III D). The $d+1$ MUBs are then explicitly exhibited. Rather interestingly, such a construction holds for every finite covariant phase space observable (SIC or otherwise). Finally we characterize SIC covariant phase space observables using the results of IV B.

In this section $\mathbb{F}$ denotes a finite field with characteristic p, different from 2. Denote by $\mathrm{Tr} : \mathbb{F} \to \mathbb{Z}_p$ the trace of $\mathbb{F}$ over the cyclic field $\mathbb{Z}_p$, and let ω be a primitive p-root of unit in $\mathbb{C}$. A reader not familiar with finite fields may wish to restrict to the case $\mathbb{F} = \mathbb{Z}_p$ with p an odd prime; in this case the trace Tr becomes the identity. This restriction does not simplify any proofs that follow and imposes undue restrictions on the dimensionality of the Hilbert space, hence we shall just consider a generic finite field $\mathbb{F}$.

Consider the vector space $V = \mathbb{F} \times \mathbb{F}$, endowed with the nondegenerate symplectic form

$$[\,\mathbf{v}\,,\,\mathbf{w}\,] = (v_2 w_1 - v_1 w_2)\,,$$

for all $\mathbf{v} = (v_1, v_2)\,,\ \mathbf{w} = (w_1, w_2)$ in V. One can think of V as a discrete phase space of a quantum system with finite degrees of freedom [6], analogous to the usual phase space $\mathbb{R}^2$ of a quantum system with continuous degrees of freedom.

For all $\mathbf{v} \in V$, the map

$$\langle\,\mathbf{v}\,,\,\cdot\,\rangle : V \to \mathbb{T} \qquad \langle\,\mathbf{v}\,,\,\mathbf{w}\,\rangle = \omega^{\mathrm{Tr}[\,\mathbf{v}\,,\,\mathbf{w}\,]}$$

defines a character of the additive abelian group V. Moreover, the map $\mathbf{v} \mapsto \langle\,\mathbf{v}\,,\,\cdot\,\rangle$ is a homomorphism of the group V into character group $\hat{V}$. Clearly, $\langle\,\mathbf{v}\,,\,\mathbf{v}\,\rangle = 1$ and $\langle\,\mathbf{v}\,,\,\mathbf{w}\,\rangle = \overline{\langle\,\mathbf{w}\,,\,\mathbf{v}\,\rangle}$ for all $\mathbf{v}, \mathbf{w} \in V$. The *symplectic Fourier transform* of V

$$\mathcal{F} : \ell^2(V) \to \ell^2(V)\,, \qquad \mathcal{F}f(\mathbf{v}) = \frac{1}{|\mathbb{F}|} \sum_{\mathbf{u} \in V} \langle\,\mathbf{v}\,,\,\mathbf{u}\,\rangle\, f(\mathbf{u})$$

is an invertible linear map with inverse

$$\mathcal{F}^{-1}\hat{f}(\mathbf{u}) = \frac{1}{|\mathbb{F}|} \sum_{\mathbf{v} \in V} \overline{\langle\,\mathbf{v}\,,\,\mathbf{u}\,\rangle}\,\hat{f}(\mathbf{v})\,.$$

We denote by S the set of 1-dimensional lines of V, i.e.,

$$\mathrm{S} = \{L \subset V \mid \mathbb{F}L = L\,,\ \dim_{\mathbb{F}} L = 1\}\,.$$

For all $\alpha \in \mathbb{F}$, let

$$L_\alpha = \mathbb{F}(1,\alpha) = \{(u,\alpha u) \mid u \in \mathbb{F}\}$$

and

$$L_\infty = \mathbb{F}(0,1) = \{(0,u) \mid u \in \mathbb{F}\}\,.$$

The following facts are easy to verify.

(a) $L_\alpha \cap L_\beta = \{\mathbf{0}\}$ for all $\alpha, \beta \in \mathbb{F} \cup \{\infty\}$ with $\alpha \neq \beta$;

(b) $V = \bigcup_{\alpha \in \mathbb{F}\cup\{\infty\}} L_\alpha$;

(c) $\mathrm{S} = \{L_\alpha \mid \alpha \in \mathbb{F} \cup \{\infty\}\}$;

(d) $|\mathrm{S}| = |\mathbb{F}| + 1$.

Hence, each $L \in \mathrm{S}$ determines an $|\mathbb{F}|$-partition of V, i.e. the set of affine lines $V/L = \{\mathbf{v} + L \mid \mathbf{v} \in V\}$ which are parallel to L. The $d+1$ partitions V/L associated with the $d+1$ lines $L \in \mathrm{S}$ share the 1-overlap property. This is due to the fact that, for $L \neq L'$, the two affine lines $\mathbf{v} + L$ and $\mathbf{u} + L'$ meet exactly at one point of V.

Let $\mathcal{H} := \ell^2(\mathbb{F})$ be the d-dimensional Hilbert space of complex functions on $\mathbb{F}$. For each $f \in \mathcal{H}$ and $\mathbf{v} = (v_1, v_2) \in V$, define the linear operator $W(\mathbf{v}) \in \mathcal{L}(\mathcal{H})$:

$$[W(\mathbf{v})f](x) := \omega^{\mathrm{Tr}[v_2(x-2^{-1}v_1)]} f(x - v_1) \qquad \forall x \in \mathbb{F}\,,$$

where 2^{-1} is the inverse of 2 in the field $\mathbb{F}$ and the action is understood to be on the left. It is an easy calculation to show that

$$W(\mathbf{v}+\mathbf{w}) = \langle \mathbf{w}, 2^{-1}\mathbf{v}\rangle W(\mathbf{v})W(\mathbf{w}) \qquad \forall \mathbf{v}, \mathbf{w} \in V\,.$$

Hence, the correspondence $\mathbf{v} \mapsto W(\mathbf{v})$ is a projective representation of V into $\mathcal{L}(\mathcal{H})$. It is called the *Weyl-Heisenberg representation* of V. The Stone-von Neumann theorem asserts that the Weyl-Heisenberg representation is essentially unique (see [23]). The following *commutation relations* are immediate

$$W(\mathbf{v})W(\mathbf{w}) = \langle\, \mathbf{v}\,,\, \mathbf{w}\,\rangle\, W(\mathbf{w})W(\mathbf{v}) \qquad \forall \mathbf{v}, \mathbf{w} \in V\,.$$

For all $L \in \mathrm{S}$, we define $|V/L| = |\mathbb{F}|$ operators by formula

$$\mathsf{P}^L(\mathbf{v}+L) = \frac{1}{|\mathbb{F}|} \sum_{\mathbf{l} \in L} \langle\, \mathbf{v}\,,\, \mathbf{l}\,\rangle\, W(\mathbf{l}) \qquad \forall \mathbf{v} + L \in V/L\,. \tag{42}$$

We then have the following facts.

Proposition 8. (i) *For all* $\mathbf{l} \in L$,

$$W(\mathbf{l}) = \sum_{\mathbf{v}+L \in V/L} \overline{\langle\, \mathbf{v}\,,\, \mathbf{l}\,\rangle} \mathsf{P}^L(\mathbf{v}+L)\,. \tag{43}$$

(ii) *For all* $\mathbf{v}, \mathbf{w} \in V$,

$$W(\mathbf{w})\mathsf{P}^L(\mathbf{v}+L)W(\mathbf{w})^* = \mathsf{P}^L(\mathbf{v}+\mathbf{w}+L)\,. \tag{44}$$

(iii) *The map* $\mathsf{P}^L : V/L \to \mathcal{L}(\mathcal{H})$ *is a PVM with* $\operatorname{rank} \mathsf{P}^L(\mathbf{v}+L) = 1$ *for all* $\mathbf{v} \in V$.

(iv) *The PVMs* $\{\mathsf{P}^L \mid L \in \mathrm{S}\}$, *are mutually unbiased.*

The proof of the above proposition, though elementary, requires some machinery. In order to keep the exposition short we refer to a forthcoming paper for its proof.

We are considering the vector space V as the phase space for a quantum system. From this perspective any POVM defined on V can be called a phase space observable. However, the most important phase space observables are covariant under the Weyl-Heisenberg representation. We say that a POVM $\mathsf{G} : V \to \mathcal{L}(\mathcal{H})$ is a *covariant phase space observable* if

$$W(\mathbf{w})\mathsf{G}(\mathbf{v})W(\mathbf{w})^* = \mathsf{G}(\mathbf{v}+\mathbf{w})$$

for all $\mathbf{v}, \mathbf{w} \in V$. It is well known [24] and easy to check in this finite dimensional case that every covariant phase space observable has the form

$$\mathsf{G}(\mathbf{v}) \equiv \mathsf{G}_T(\mathbf{v}) := \frac{1}{|\mathbb{F}|} W(\mathbf{v}) T W(\mathbf{v})^*$$

for a unique operator $T \geq 0$ with $\mathrm{tr}\,[T] = 1$.

For any line $L \in \mathrm{S}$, we define the *L-marginal of* G_T by

$$\mathsf{G}_T^L(\mathbf{v}+L) = \sum_{\mathbf{l} \in L} \mathsf{G}_T(\mathbf{v}+\mathbf{l}) \qquad \forall \mathbf{v}+L \in V/L\,. \tag{45}$$

It is clear that $\mathsf{G}_T^L(\mathbf{v}+L) \geq 0$ and $\sum_{\mathbf{v}+L\in V/L} \mathsf{G}_T^L(\mathbf{v}+L) = I$, hence G_T^L is a POVM on V/L. We further observe that G_T^L satisfies the same covariance properties as P^L, i.e.,

$$W(\mathbf{w})\mathsf{G}_T^L(\mathbf{v}+L)W(\mathbf{w})^* = \mathsf{G}_T^L(\mathbf{v}+\mathbf{w}+L)$$

for all $\mathbf{v}, \mathbf{w} \in V$. In particular,

$$[\mathsf{G}_T^L(\mathbf{v}+L)\,,\, W(\mathbf{l})] = 0 \tag{46}$$

for all $\mathbf{v} \in V$ and $\mathbf{l} \in L$.

Theorem 4. *Suppose* $T \geq 0$ *with* $\mathrm{tr}\,[T] = 1$, *and let* G_T *be the corresponding covariant phase space observable.*

(a) *For each* $L \in \mathrm{S}$, *the L-marginal* G_T^L *of* G_T *is a smearing of* P^L. *More precisely, for all* $\mathbf{v} \in V$,

$$\mathsf{G}_T^L(\mathbf{v}+L) = \sum_{\mathbf{w}+L\in V/L} \Lambda_T^L(\mathbf{v}-\mathbf{w}+L)\mathsf{P}^L(\mathbf{w}+L)\,, \tag{47}$$

where $\Lambda_T^L : V/L \to [0,1]$ *is the probability measure*

$$\Lambda_T^L(\mathbf{v}+L) = \mathrm{tr}\left[T\mathsf{P}^L(-\mathbf{v}+L)\right]\,. \tag{48}$$

(b) *The* $|\mathbb{F}|+1$ *POVMs* $\{\mathsf{G}_T^L \mid L \in \mathrm{S}\}$ *are mutually unbiased.*

Proof. (a) By (46) and the definition of P^L, we have

$$[\mathsf{G}_T^L(\mathbf{v}+L)\,,\, \mathsf{P}^L(\mathbf{w}+L)] = 0 \qquad \forall \mathbf{w} \in V\,,$$

hence, in view of item (iii) of Proposition 8,

$$\mathsf{G}_T^L(\mathbf{v}+L) = \sum_{\mathbf{w}+L\in V/L} K(\mathbf{v}+L, \mathbf{w}+L)\mathsf{P}^L(\mathbf{w}+L) \quad \forall \mathbf{v} \in V$$

for some function $K : V/L \times V/L \to \mathbb{C}$. Next, we have:

$$K(\mathbf{v}+L,\mathbf{w}+L)=\mathrm{tr}\left[\mathsf{G}_T^L(\mathbf{v}+L)\mathsf{P}^L(\mathbf{w}+L)\right]=\frac{1}{|\mathbb{F}|}\sum_{\mathbf{l}\in L}\mathrm{tr}\left[TW(\mathbf{v}+\mathbf{l})^*\mathsf{P}^L(\mathbf{w}+L)W(\mathbf{v}+\mathbf{l})\right].$$

Using (44) this reduces to

$$K(\mathbf{v}+L,\mathbf{w}+L)=\mathrm{tr}\left[T\mathsf{P}^L(\mathbf{w}-\mathbf{v}+L)\right]\equiv\Lambda_T^L(\mathbf{v}-\mathbf{w}+L)\,.$$

(b) If $L_1,L_2\in\mathrm{S}$, with $L_1\neq L_2$, then, for all $\mathbf{v}_1,\mathbf{v}_2\in V$,

$$\mathrm{tr}\left[\mathsf{G}_T^{L_1}(\mathbf{v}_1+L_1)\mathsf{G}_T^{L_2}(\mathbf{v}_2+L_2)\right]=\frac{1}{|\mathbb{F}|}\sum_{\mathbf{w}_1+L_1\in V/L_1}\sum_{\mathbf{w}_2+L_2\in V/L_2}\Lambda_T^{L_1}(\mathbf{v}_1-\mathbf{w}_1+L_1)\Lambda_T^{L_2}(\mathbf{v}_2-\mathbf{w}_2+L_2)=\frac{1}{|\mathbb{F}|}\,,$$

where the first equality arises from the use of item (iv) of Proposition 8, and the final equality is due to $\Lambda_T^{L_i}$ $(i=1,2)$ being probability measures. □

At this point, we recall the qubit example discussed in Section II C. If we start from three mutually unbiased POVMs $\mathsf{P}^k(\pm)=\frac{1}{2}(I\pm\boldsymbol{n}_k\cdot\boldsymbol{\sigma})$, where the vectors $\boldsymbol{n}_1$, $\boldsymbol{n}_2$ and $\boldsymbol{n}_3$ are orthogonal unit vectors, then it is straightforward to verify that a covariant phase space observable G_T is a SIC if the generating operator T, now thought of as a state, is rank-1 and satisfies

$$\mathrm{tr}\left[T\boldsymbol{n}_1\cdot\boldsymbol{\sigma}\right]=\mathrm{tr}\left[T\boldsymbol{n}_2\cdot\boldsymbol{\sigma}\right]=\mathrm{tr}\left[T\boldsymbol{n}_3\cdot\boldsymbol{\sigma}\right]\,. \tag{49}$$

This condition simply means that the expectations values of the state T in the measurements of P^1, P^2 and P^3 are equal.

We are aiming for a comparable condition in the odd prime power dimensions, but now have to look for more complicated measurements than just P^L. For all $L\in\mathrm{S}$, we define the PVM $\mathsf{Q}^L:V/L\to\mathcal{L}(\mathcal{H}\otimes\mathcal{H})$ by

$$\mathsf{Q}^L(\mathbf{u}+L)=\sum_{\mathbf{w}\in V/L}\mathsf{P}^L(\mathbf{u}+\mathbf{w}+L)\otimes\mathsf{P}^L(\mathbf{w}+L)\,.$$

The measurement outcome distribution of Q^L gives the difference of two P^L-measurements performed on two identical systems.

The following is the main result of the section.

Theorem 5. *Suppose $T\geq 0$ with $\mathrm{tr}\left[T\right]=1$, and let G_T be the corresponding covariant phase space observable. The following facts are equivalent:*

(i) *G_T is SIC;*

(ii) $\mathrm{tr}\left[\mathsf{G}_T^L(\mathbf{v}+L)\mathsf{G}_T^L(\mathbf{w}+L)\right]=(1+\delta_{\mathbf{v}+L,\mathbf{w}+L})/(|\mathbb{F}|+1)$ *for all $L\in\mathrm{S}$ and $\mathbf{v},\mathbf{w}\in V$;*

(iii) $\mathrm{tr}\left[(T\otimes T)\mathsf{Q}^L(\mathbf{v}+L)\right]=(1+\delta_{\mathbf{v}+L,\mathbf{0}+L})/(|\mathbb{F}|+1)$ *for all $L\in\mathrm{S}$ and $\mathbf{v}\in V$;*

(iv) $|\mathrm{tr}\left[TW(\mathbf{v})\right]|^2=(1+|\mathbb{F}|\delta_{\mathbf{v},\mathbf{0}})/(|\mathbb{F}|+1)$ *for all $\mathbf{v}\in V$.*

Proof. (i) ⇔ (ii) If G_T is SIC, item (ii) follows at once from equations (20) and (21) in Theorem 1.
For the converse implication notice that, by item (b) of Theorem 4, the $d+1$ marginals G_T^L of a generic phase space observable G_T are mutually unbiased. If G_T also satisfies item (ii), the hypothesis of Theorem 3 are met. Hence the operators

$$\frac{1}{d}\left(\sum_{L\in\mathrm{S}}\mathsf{G}_T^L(\mathbf{v}+L)-I\right)$$

form a SIC system that, by Proposition 6, coincides with the phase space observable G_T.

(ii) ⇔ (iii) This is a consequence of

$$\begin{aligned}&\mathrm{tr}\left[\mathsf{G}_T^L(\mathbf{v}+L)\mathsf{G}_T^L(\mathbf{w}+L)\right]\\&\quad=\sum_{\mathbf{u}+L\in V/L}\Lambda_T^L(\mathbf{u}+\mathbf{w}-\mathbf{v}+L)\Lambda_T^L(\mathbf{u}+L)\\&\quad=\mathrm{tr}\left[(T\otimes T)\mathsf{Q}^L(\mathbf{v}-\mathbf{w}+L)\right]\,.\end{aligned}$$

(iii) ⇔ (iv) For all $\mathbf{v}\in V$, setting $L=\mathbb{F}\mathbf{v}$, we have

$$\begin{aligned}&\frac{1}{|\mathbb{F}|}\sum_{\mathbf{u}\in V}\langle\,\mathbf{v}\,,\,\mathbf{u}\,\rangle\,\mathsf{Q}^L(\mathbf{u}+L)=\sum_{\mathbf{u}+L\in V/L}\langle\,\mathbf{v}\,,\,\mathbf{u}\,\rangle\,\mathsf{Q}^L(\mathbf{u}+L)\\&=\sum_{\mathbf{u}+L,\,\mathbf{w}+L\in V/L}\langle\,\mathbf{v}\,,\,\mathbf{u}\,\rangle\,\mathsf{P}^L(\mathbf{u}+\mathbf{w}+L)\otimes\mathsf{P}^L(\mathbf{w}+L)\\&\text{(changing }\mathbf{u}+L\to\mathbf{u}-\mathbf{w}+L)\\&=\sum_{\mathbf{u}+L,\,\mathbf{w}+L\in V/L}\langle\,\mathbf{v}\,,\,\mathbf{u}\,\rangle\,\overline{\langle\,\mathbf{v}\,,\,\mathbf{w}\,\rangle}\mathsf{P}^L(\mathbf{u}+L)\otimes\mathsf{P}^L(\mathbf{w}+L)\\&\text{(by (43))}\\&=W(\mathbf{v})\otimes W(\mathbf{v})^*\,.\end{aligned}$$

Therefore,

$$\frac{1}{|\mathbb{F}|}\sum_{\mathbf{u}\in V}\langle\,\mathbf{v}\,,\,\mathbf{u}\,\rangle\,\mathrm{tr}\left[(T\otimes T)\mathsf{Q}^L(\mathbf{u}+L)\right]=|\mathrm{tr}\left[TW(\mathbf{v})\right]|^2\,,$$

and the equivalence of (iii) and (iv) follows by symplectic Fourier transform for the group V. □

A condition equivalent to (iii) in Theorem 5 was already established in [25] (see equation (17) there). The part of this condition that we would have anticipated after the qubit example is that the numerical values of the probabilities $\mathrm{tr}\left[(T\otimes T)\mathsf{Q}^L(\cdot)\right]$ are the same for all $L \in \mathrm{S}$. It would be interesting to find a physical explanation for the mathematical fact that the correct values are the ones given in (iii) in Theorem 5.

VII. CONCLUSION

We have obtained an interesting, if incomplete, connection between SICs and MUBs that is based on an operational feature, namely joint measurability. The results of sections III and IV can be summarized as follows:

(a) For a SIC G we may form n d-partitions of G that satisfy the 1-overlap property; the number n is equal to 2 + the maximum number of mutually orthogonal Latin squares of order d. The partitions induce n marginal POVMs which are mutually unbiased with respect to each other.

If the elements of each marginal POVM commute with each other, the marginals are smearings of spectral measures whose (rank-1) projections correspond to a system of n MUBs.

(b) From a complete set of $d+1$ MUBs one can construct $d+1$ commutative POVMs by smearing the corresponding PVMs, and via suitable smearings these POVMs are mutually unbiased. By assuming that each mutually unbiased POVM element is the sum of d operators $\mathsf{G}(i)$ out of a set $\{\mathsf{G}(i)\}_{i=0}^{d^2-1}$ such that no two elements from the same POVM share an operator, and any two elements from different POVMs share only one, one can show that the operators $\mathsf{G}(i)$ form a SIC system, that is they satisfy all properties of a SIC with the possible exception of positivity, which does not follow naturally.

With these findings we have established the beginnings of a correspondence between a SIC and a complete set of $d+1$ MUBs. The bridge providing this connection is provided by the concept of a complete system of mutually unbiased POVMs that will be marginals of the SIC. There are, however, obstructions to the existence of this bridge.

First, the number of mutually unbiased POVMs that can be obtained as marginals of a SIC is no less than 3 but also no greater than 2 plus the maximal number of orthogonal Latin squares of order d. The maximal number of mutually unbiased POVMs will thus be $d+1$ when d is a prime power, but it is unknown whether this number can be obtained for any other values of d.

Second, the problem remains of extracting MUBs from such a system of mutually unbiased POVMs; we have obtained a solution only in the case where all the POVMs are commutative.

Third, starting with a system of $d+1$ MUBs (where they exist), one can obtain $d+1$ mutually unbiased POVMs by applying an appropriate smearing by application of a doubly stochastic matrix to the spectral measures associated with the MUBs. However, in order to reconstruct a SIC via the formula (36), it is required that for the underlying $(d+1)\times d$ array there exist d^2 downward paths of length d which satisfy the 1-overlap property – this was found again to be equivalent to the requirement that there are $d-2$ orthogonal Latin squares of order d.

To illustrate the significance of these limitations, we revisit the case of a 6-dimensional Hilbert space. In this case there do not exist two mutually orthogonal Latin squares of order 6, and so there are no systems of mutually unbiased marginals of a SIC with more than 3 elements. As a consequence of Proposition 5, since there do not exist seven 6-partitions with the 1-overlap property in a 6×6 array, there cannot exist 36 downward paths with the 1-overlap property in a 7×6 array. So even if we hypothesized the existence of 7 MUBs for $d=6$, it is impossible to construct a SIC from them via formula (36), although SICs are known to exist for $d=6$ [7].

To summarize: The existence in $\mathcal{H}_d$ of a bridge between a complete system of MUBs and a SIC via mutually unbiased POVMs and the formula (36) requires the existence of the maximal number $d-1$ of mutually orthogonal Latin squares.

But even when the conditions of the recovery of a SIC system from a system of $d+1$ mutually unbiased POVMs are fulfilled, the problem remains of ensuring the positivity of the operators $\mathsf{G}(i)$, $i=1,\ldots,d^2$. By construction, these operators satisfy $\mathrm{tr}\left[d\mathsf{G}(i)\right]=1$ and $\mathrm{tr}\left[(d\mathsf{G}(i))^2\right]=1$. Using an observation made in [26], the operators $d\mathsf{G}(i)$ are positive (and in fact rank-1 projections) if, in addition, $\mathrm{tr}\left[(d\mathsf{G}(i))^3\right]=1$.

The positivity of the SIC system elements depend on the doubly stochastic matrices Λ^k used in smearing our mutually unbiased spectral measures, but these pose their own set of problems. By demanding that their coefficients are positive (and hence real) and less than or equal to 1, and that their rows satisfy conditions (26a) and (26b), we are able to drastically reduce the number of degrees of freedom. Indeed, if we simplify the situation by further requiring that the rows of a given doubly stochastic matrix Λ^k, whose rows satisfy (26a) and (26b), are given as cyclic permutations of the elements in the first row, then the entire matrix is determined by a single element of this row, with all other elements of the matrix arising as a result. However, the value of this variable lies within a continuous interval, and no particular value need immediately stand out as significant. Further to this, it is not known beforehand how many different doubly stochastic matrices need to be used - that is, how many spectral measures are smeared in the same way and how many require a different smearing - in order to retrieve a SIC POVM (in the case of a SIC system, a single matrix - that is, all spectral measures are smeared

in the same way - will suffice). The issue of the number of paths does not need discussion here; given that there are d^{d+1} possible downwards paths through a $(d+1)\times d$ array, as described in section IV (excluding the 1-overlap property here), it is computationally simple to perform a check of all possible paths to see if they form positive operators.

As an example of these issues, in the case of $d = 3$, where we begin with 4 mutually unbiased spectral measures, there are several possible doubly stochastic matrices, of which we choose one, that can be used on 3 of the spectral measures, and then the fourth measure must be smeared by the doubly stochastic matrix whose first row is $(1/2, 1/2, 0)$ and whose remaining rows are cyclic permutations of this. It is also the case that this doubly stochastic matrix can be used on all four mutually unbiased spectral measures and will still lead to a SIC POVM.

The SIC–MUB bridge constructed here is based on two combinatorial schemes that were noted to be equivalent; we showed that this dual combinatorial structure corresponds one-to-one to a dual geometric structure of affine planes that was posited in a study of Wootters [2] in which he laid out analogous schemes for constructing MUBs and SICs. The operator systems needed to start Wootters' schemes are not given *a priori* while in our approach these operators were given and the geometric/combinatorial structures appeared by necessity.

Finally, in Section VI we showed that all these facts find a natural application to finite covariant phase space observables in prime power dimension $d = p^n$ ($p \neq 2$). Indeed, it turns out that a covariant phase space observable on a d-dimensional Hilbert space generates $d+1$ mutually unbiased and commutative marginal POVMs, which in turn are smearings of $d+1$ MUBs. Such marginal POVMs are associated to each d-partition of the finite phase space into parallel affine lines. Moreover, in Theorem 5, we provided various characterizations of SIC covariant phase space observables; in particular, item (iii) establishes an operational link between the SIC property of the covariant phase space observable G_T and the $d+1$ MUBs associated with the $d+1$ mutually unbiased marginal POVMs of G_T.

ACKNOWLEDGEMENTS

T.B. and P.B. gratefully acknowledge support through the White Rose Studentship Network *Optimising Quantum Processes and Quantum Devices for future Digital Economy Applications*, which provided funds for a studentship and mutual visits between the project partners. T.H. acknowledges support from the Academy of Finland (grant no.138135). A. T. gratefully acknowledges the financial support of the Italian Ministry of Education, University and Research (FIRB project RBFR10COAQ).

[1] M. Grassl, On SIC-POVMs and MUBs in dimension 6. *arXiv:quant-ph/0406175* (2004).

[2] W.K. Wootters. Quantum measurements and finite geometry. *Found. Phys.* **36**,112–126 (2006).

[3] S. Gurevich, R. Hadani, N. Sochen, The finite harmonic oscillator and its applications to sequences, communication, and radar. *IEEE Trans. Inform. Theory* **54**, 4239–4253 (2008),

[4] G. Zauner, Quantum designs–foundations of a noncommutative design theory. *Int. J. Quantum Inf.* **9**, 445–507 (2011), originally published in German in 1999 as Ph.D. Thesis, University of Vienna.

[5] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, F. Vatan, A new proof for the existence of mutually unbiased bases. *Algorithmica* **34**, 512–528 (2002).

[6] K.S. Gibbons, M.J. Hoffman, W.K. Wootters, Discrete phase space based on finite fields. *Phys. Rev. A* **70**, 062101 (2004).

[7] J.M. Renes, R. Blume-Kohout, A.J. Scott, C.M. Caves, Symmetric informationally complete quantum measurements. *J. Math. Phys.* **45**, 2171–2180 (2004).

[8] M. Saniga, M. Planat, H. Rosu, Mutually unbiased bases and finite projective planes. *J. Optics B: Quant. Semiclass. Opt.* **6** ,L19 (2004).

[9] R. Howe, Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries. *Indag. Math. (N.S.)* **16**, 553–583 (2005).

[10] D.M. Appleby, SIC-POVMs and MUBs: geometric relationships in prime dimension. *arXiv:0905.1428* (2009).

[11] T. Paterek, B. Dakić, Č. Brukner, Mutually unbiased bases, orthogonal latin squares, and hidden-variable models. *Phys. Rev. A* **79**, 012109 (2009).

[12] T. Durt, B.-G. Englert, I. Bengtsson, K. Życzkowski, On mutually unbiased bases. *Int. J. Quantum Inf.* **8**, 535–640 (2010).

[13] A. J. Scott and M. Grassl, Symmetric informationally complete positive-operator-valued measures: A new computer study. *J. Math. Phys.* **51**, 042203 (2010).

[14] M. Revzen, Radon transform in finite Hilbert space *Europhys. Lett* **98**, 10001 (2012).

[15] A. Klappenecker, M. Rötteler, Constructions of mutually unbiased bases. In: G.L. Mullen, A. Poli, and H. Stichtenoth, editors, *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Computer Science*, pp. 137–144. Springer Berlin Heidelberg, 2004.

[16] W.K. Wootters, B.D. Fields, Optimal state-determination by mutually unbiased measurements. *Ann. Phys. (N.Y.)* **191**, 363–381 (1989).

[17] P. Butterley, W. Hall, Numerical evidence for the maximum number of mutually unbiased bases in dimension six. *Phys. Lett. A* **369**, 5–8 (2007).

[18] S. Colin, J. Corbett, T. Durt, D. Gross, About SIC POVMs and discrete Wigner distributions and discrete Wigner distributions. *J. Optics B: Quant. Semiclass. Opt.* **7**, S778 (2005).

[19] D.M. Appleby, I. Bengtsson, S. Brierley, M. Grassl, D. Gross, J.-Å. Larsson, The monomial representations of the Clifford group. *Quant. Inf. Comput.* **12**, 0404–0431

(2012) (*arXiv:1102.1268v2*).

[20] D.M. Appleby, I. Bengtsson, S. Brierley, Å. Ericsson, M. Grassl, J.-Å. Larsson Systems of Imprimitivity for the Clifford Group. *arXiv:1210.1055* (2012).

[21] M. Hartmann, *private communication* (2012).

[22] D.R. Stinson, A short proof of the nonexistence of a pair of orthogonal latin squares of order six. *J. Combin. Th., Ser. A* **36**, 373 – 376 (1984).

[23] G.W. Mackey, A theorem of Stone and von Neumann. *Duke Math. J.* **16**, 313–326, 1949.

[24] A.S. Holevo, Covariant measurements and uncertainty relations. *Rep. Math. Phys.* **16**, 385–400 (1979).

[25] D. M. Appleby, H. B. Dang, C. A. Fuchs, Symmetric informationally-complete quantum states as analogues to orthonormal bases and minimum-uncertainty states. *arXiv:0707.2071* (2007).

[26] N.S. Jones, N. Linden, Parts of quantum states. *Phys. Rev. A* **71**, 012324 (2005).