Informational power of the Hoggar symmetric informationally complete positive operator-valued measure

Anna Szymusiak* and Wojciech Słomczyński†
Institute of Mathematics, Jagiellonian University, Łojasiewicza 6, 30-348 Kraków, Poland
(Received 29 April 2016; published 29 July 2016)

We compute the informational power for the Hoggar symmetric informationally complete positive operator-valued measure (SIC-POVM) in dimension eight, i.e., the classical capacity of a quantum-classical channel generated by this measurement. We show that the states constituting a maximally informative ensemble form a twin Hoggar SIC-POVM being the image of the original one under a conjugation.

DOI: 10.1103/PhysRevA.94.012122

I. INTRODUCTION

Among positive operator-valued measures (POVMs) representing general quantum measurements, symmetric informationally complete (SIC) POVMs, called "mysterious entities" by Fuchs [1], play a special role. On the one hand, they are crucial ingredients of the quantum Bayesianism (or QBism) approach to the foundations of quantum physics proposed 15 years ago by Caves, Fuchs, and Schack [2–4]; on the other hand, they are widely used in various areas of quantum information theory like quantum cryptography [5], quantum state tomography [6–9], quantum communication [10], and entanglement detection [11] (see [12,13] for more applications).

However, despite many efforts as well as positive results obtained for lower dimensions (see, e.g., [12,14] and [15, Appendix B]), these important objects remain elusive, as the problem of their existence in arbitrary dimension is still open. Recently, this question has been reformulated in the language of various algebraic structures (Lie groups, Lie algebras, and Jordan algebras) [16], but it has also a simple interpretation in terms of metric spaces. Namely, the existence of SIC-POVMs in dimension d is equivalent to the fact that the equilateral dimension (i.e., the maximum number of equidistant points) [17,18] of the d-dimensional complex projective space endowed with the Fubini-Study metric equals d^2.

The eight-dimensional Hoggar lines [19] provide one of the first examples of SIC-POVMs found in dimension larger than two. It seems that this set exhibits a higher level of symmetry than most known SIC-POVMs and, at the same time, its symmetry has a slightly different character than in the case of all other known SIC-POVMs. This—using Blakean language—"fearful symmetry" of Hoggar lines makes it an especially interesting object of study.

The informational power of a quantum measurement, that is, the maximum amount of classical information that it can extract from any ensemble of quantum states [20], being equal to the classical capacity of a quantum-classical channel generated by this measurement, has received much attention in recent years [10,21–27]. However, this quantity is in general not easy to compute analytically, especially in higher dimensions. In this paper we show that the informational power of the Hoggar SIC-POVM is equal to $2\ln(4/3)$. To this aim we use the construction of Hoggar lines newly discovered by Jedwab and Wiebe [28]. As a corollary we get that the bound for the informational power of 2-designs (including SIC-POVMs) obtained recently by Dall'Arno [26] is saturated in dimension eight. Moreover, we show that a maximally informative ensemble for a Hoggar SIC-POVM forms another "twin" Hoggar SIC-POVM that is the image of the original one under a (complex) conjugation, i.e., an antiunitary involutive map, and sharing the same symmetries as the original one.

II. SIC-POVMs

With any finite-dimensional quantum system one can associate a complex Hilbert space $\mathbb{C}^d$. Then the pure states $\mathcal{P}(\mathbb{C}^d)$ of the system are described by one-dimensional orthogonal projections, i.e., $\mathcal{P}(\mathbb{C}^d) := \{\rho \in \mathcal{L}(\mathbb{C}^d) | \rho \geqslant 0, \rho^2 = \rho, \operatorname{tr}(\rho) = 1\}$, and the mixed states $\mathcal{S}(\mathbb{C}^d)$ are convex combinations of pure states, that is, density operators on $\mathbb{C}^d$.

A general quantum measurement is described by a *positive operator valued measure* (*POVM*). In this paper we consider the discrete version of it; i.e., by POVM we mean a set $\Pi := \{\Pi_j\}_{j=1}^k$ of nonzero positive semidefinite operators on $\mathbb{C}^d$ satisfying the identity decomposition $\sum_{j=1}^k \Pi_j = \mathrm{I}_d$. In this framework the probability of obtaining the jth ($j = 1,\dots,k$) outcome, given that the initial (premeasurement) state of the system was $\rho \in \mathcal{S}(\mathbb{C}^d)$, is equal to $p_j(\rho,\Pi) := \operatorname{tr}(\rho\Pi_j)$.

Among quantum measurements we can distinguish *symmetric informationally complete* (SIC) POVMs, i.e., POVMs consisting of d^2 subnormalized rank-one projectors $\Pi_j := |\phi_j\rangle\langle\phi_j|/d$ ($j = 1,\dots,k$) with equal pairwise Hilbert-Schmidt inner products: $\operatorname{tr}(\Pi_i\Pi_j) = |\langle\phi_i|\phi_j\rangle|^2/d^2 = 1/[d^2(d+1)]$ for $i \neq j$, $i,j = 1,\dots,k$, where ϕ_j are elements of the unit sphere in $\mathbb{C}^d$ determined up to a phase factor. Note that this condition implies that SIC-POVMs are indeed *informationally complete* (*IC*); i.e., the statistics of measurement uniquely determine the initial state [29]. Since any IC-POVM must contain at least d^2 elements, SIC-POVMs are special examples of *minimal* IC-POVMs. If the premeasurement pure state is given by $|\psi\rangle\langle\psi|$, where ψ is an element of the unit sphere in $\mathbb{C}^d$, then $p_j(|\psi\rangle\langle\psi|,\Pi) = |\langle\psi|\phi_j\rangle|^2/d$.

Furthermore, let us recall that a *complex projective t-design* ($t \in \mathbb{N}$) is a set $\{\rho_j\}_{j=1}^k$ of pure states such that

$$\frac{1}{k^2}\sum_{j,m=1}^{k} f(\operatorname{tr}(\rho_j\rho_m)) = \iint_{\mathcal{P}(\mathbb{C}^d)\times\mathcal{P}(\mathbb{C}^d)} f(\operatorname{tr}(\rho\sigma))\,d\mu(\rho)\,d\mu(\sigma)$$

*anna.szymusiak@uj.edu.pl
†wojciech.slomczynski@im.uj.edu.pl

for every real-valued polynomial f of degree t or less, where μ stands for the unique unitarily invariant (Fubini-Study) probabilistic measure on $\mathcal{P}(\mathbb{C}^d)$ [6]. The SIC-POVMs can be equivalently described as complex projective 2-designs (called also *spherical quantum* 2-*designs*) with d^2 elements; see, e.g., [29].

III. INFORMATIONAL POWER

The indeterminacy of quantum measurement $\Pi := \{\Pi_j\}_{j=1}^k$ can be quantized by a number that characterizes the randomness of the distribution of measurements outcomes $(p_j(\rho,\Pi))_{j=1}^k$ depending on the premeasurement state of the system, $\rho \in \mathcal{S}(\mathbb{C}^d)$. The most natural choice for such a tool is the *Shannon entropy*. Thus, by the *entropy of the measurement* Π we mean a function $H(\cdot,\Pi) : \mathcal{S}(\mathbb{C}^d) \to \mathbb{R}$ defined by

$$H(\rho,\Pi) := \sum_{j=1}^{k} \eta(p_j(\rho,\Pi)),$$

where the *Shannon entropy function* $\eta : [0,1] \to \mathbb{R}$ is given by $\eta(t) := -t \ln t$ for $t > 0$ and $\eta(0) := 0$; see [27] for the history and interpretation of this notion. It follows from the concavity of H that this function attains minima in the set of pure states; finding the minimizers, however, is not a trivial task in general, even for SIC-POVMs, where only the results for dimensions two [10,27] and three [25] are known. In fact, the latter result was proven under the assumption that a SIC-POVM is covariant, but it follows from [18] that all SIC-POVMs in dimension three share this property. On the other hand, for an arbitrary SIC-POVM, the maximum value of H for pure premeasurement states is equal to $[(d-1)/d] \ln(d+1)$ [30].

Let us now consider an ensemble $\mathcal{E} = (\tau_i, p_i)_{i=1}^m$, where $p_i \geqslant 0$ are *a priori* probabilities of density matrices $\tau_i \in \mathcal{S}(\mathbb{C}^d)$, for $i = 1,\dots,m$, and $\sum_{i=1}^m p_i = 1$. The *mutual information* between $\mathcal{E}$ and Π is given by

$$I(\mathcal{E},\Pi) := \sum_{i=1}^{m} \eta\left(\sum_{j=1}^{k} P_{ij}\right) + \sum_{j=1}^{k} \eta\left(\sum_{i=1}^{m} P_{ij}\right) - \sum_{i=1}^{m}\sum_{j=1}^{k} \eta(P_{ij}),$$

where $P_{ij} := p_i \operatorname{tr}(\tau_i \Pi_j)$ for $i = 1,\dots,m$ and $j = 1,\dots,k$. This quantity can be considered as a measure of how much information can be extracted from ensemble $\mathcal{E}$ by measurement Π. Thus the following two questions arise: what is the maximum amount of information one can get from the given ensemble (i.e., $\max_\Pi I(\mathcal{E},\Pi)$, studied, e.g., in [31–33]) and what is the capability of extracting information by given measurement (i.e., $\max_{\mathcal{E}} I(\mathcal{E},\Pi)$, examined in [10,20,21,23,27])? The latter quantity, denoted by $W(\Pi)$, is called the *informational power* of Π.

Both the minimum entropy and the informational power of Π can also be interpreted in terms of the *quantum-classical channel* $\Phi : \mathcal{S}(\mathbb{C}^d) \to \mathcal{S}(\mathbb{C}^k)$ generated by Π and given by $\Phi(\rho) := \sum_{j=1}^k \operatorname{tr}(\rho \Pi_j)|e_j\rangle\langle e_j|$ for some orthonormal basis $(|e_j\rangle)_{j=1}^k$ in $\mathbb{C}^k$. The former quantity is equal to the *minimum output entropy* of Φ, $\min_\rho S(\Phi(\rho))$, where S is the *von Neumann entropy* defined by $S(\tau) := -\operatorname{tr}(\tau \ln \tau)$ for $\tau \in \mathcal{S}(\mathbb{C}^d)$ [34]. The latter one is just the *classical capacity* $\chi(\Phi)$ of the channel Φ, given by $\chi(\Phi) := \max_{\mathcal{E}=(\tau_i,p_i)_{i=1}^m} \{S(\sum_{i=1}^m p_i \Phi(\tau_i)) - \sum_{i=1}^m p_i S(\Phi(\tau_i))\}$ [10,22].

The minimal entropy of Π and its informational power are related by

$$W(\Pi) \leqslant \ln k - \min_{\rho \in \mathcal{S}(\mathbb{C}^d)} H(\rho,\Pi) \tag{1}$$

and the equality holds if and only if there exists an ensemble $\mathcal{E} = (p_i,\tau_i)_{i=1}^m$ such that the states τ_i $(i = 1,\dots,m)$ are minimizers of $H(\cdot,\Pi)$ and $\operatorname{tr}[(\sum_{i=1}^m p_i \tau_i)\Pi_j] = 1/k$ for $j = 1,\dots,k$ (Proposition 6 of [27]). This condition is in particular fulfilled if we assume that Π is covariant with respect to an irreducible representation, a fact already observed by Holevo [35]. To see this, it is enough to consider the ensemble consisting of equiprobable elements of the orbit of any minimizer of H under the action of this representation.

So far the informational power has been computed analytically in few cases only: for all highly symmetric POVMs in dimension two, namely seven sporadic measurements, including the "tetrahedral" SIC-POVM, and one infinite series [27] (though for some of them the result was known earlier; see [10,21,36–38]), the SIC-POVMs in dimension three [25], and the POVMs consisting of four mutually unbiased bases (MUBs), again in dimension three [24]. The first two results have been obtained with the method developed in [27] based on the Hermite interpolation of the Shannon entropy function. In this paper we enlarge this collection, computing the informational power for the Hoggar SIC-POVM.

Let us recall that for SIC-POVMs in dimension d the sum of squared probabilities of the measurement outcomes (the so-called *index of coincidence*, known under various names in the literature; see Sec. 8 of [39]) is the same for each initial pure state and equal to $r := 2/[d(d+1)]$. The problem of finding the minimum of the Shannon entropy under the assumption that the index of coincidence is equal to r was analyzed by Harremoës and Topsøe (Theorem 2.5 in [40]; see [41] for further discussion). From their result one can deduce that if $1/r \in \mathbb{N}$, then this minimum is attained for the probability distribution $(r,\dots,r,0,\dots,0)$ with $1/r$ probabilities equal to r, and the rest equal to zero. Hence, the minimum entropy of a SIC-POVM is bounded from below by $\ln(d(d+1)/2)$, and using inequality (1) with $k = d^2$, we get that its informational power is bounded from above by $\ln(2d/(d+1))$ (see also Corollary 2 of [26]). The achievability of this bound in dimension d is equivalent to the existence of a vector (representing a pure state) orthogonal to $(d-1)d/2$ elements of a SIC-POVM, and making equal angles with $d(d+1)/2$ others, the problem already analyzed in [3]. Consequently, this bound is achieved for SIC-POVMs in dimensions two and three, but numerical results suggest that this is not the case for known SIC-POVMs in dimensions four and five [3,26]. We shall see that this bound is achieved again in dimension eight for the Hoggar SIC-POVM.

IV. HOGGAR LINES AND THEIR SYMMETRIES

The *Hoggar (lines)* SIC-POVM (HL) was constructed with the help of computer by Hoggar in [19] as the complexification of 64 lines through the origin in the four-dimensional quaternionic space or, more precisely, as the set of diameters of a quaternionic polytope with 128 vertices. In fact, he had announced this result as early as in [42], and in [43] gave a computer-independent proof that these lines are equiangular. One year later, Zauner showed in his thesis [44] that this SIC-POVM is covariant with respect to P_3, the quotient of the *three-qubit Pauli group* (called also the *Galoisian variant of the discrete Weyl-Heisenberg group in dimension eight*) by its center. This group can be obtained as the projective unitary representation of $\mathbb{Z}_2^3 \otimes \mathbb{Z}_2^3$ given by the operators $Z^{\alpha_1} X^{\beta_1} \otimes Z^{\alpha_2} X^{\beta_2} \otimes Z^{\alpha_3} X^{\beta_3}, \alpha,\beta \in \mathbb{Z}_2^3$, with $X|e_j\rangle := |e_{j\oplus 1}\rangle$ and $Z|e_j\rangle := (-1)^j |e_j\rangle$ for $j = 0,1$, where $\{e_0,e_1\}$ is an orthonormal basis in $\mathbb{C}^2$. Quite recently, Zhu (Sec. 12 in [12]) proved the long-expected result that the Hoggar lines are not projectively equivalent to any SIC-POVM covariant with respect to the group $\mathbb{Z}_8 \otimes \mathbb{Z}_8$ isomorphic to the quotient of the usual discrete Weyl-Heisenberg group in dimension eight by its center. As the Hoggar SIC-POVM is currently the only known such example in any dimension, this property makes this object exceptional among SIC-POVMs [15]. In the present paper, by a Hoggar SIC-POVM we mean any SIC-POVM projectively equivalent to the original Hoggar construction.

In his thesis (Sec. 10.4 in [12]), Zhu analyzed the extended symmetry group of the Hoggar lines, $\mathrm{Sym}\,(HL)$, i.e., the subgroup of the projective unitary-antiunitary group $\mathrm{PUA}\,(\mathbb{C}^8)$ leaving this set invariant, and showed that it has 774 144 elements. Zhu proved also that $\mathrm{Sym}\,(HL)$ is a subgroup of the *extended multiqubit Clifford collineation group* $\overline{\mathcal{EC}}(8)$ of the three-qubit Pauli group, i.e., its normalizer within $\mathrm{PUA}\,(\mathbb{C}^8)$, having $240 \times 774\,144$ elements. Analogously, the unitary symmetry group of the Hoggar lines $\mathrm{Sym}_U\,(HL)$ is a subgroup of order 387 072 of the *multiqubit Clifford collineation group* $\overline{\mathcal{C}}(8)$ with $240 \times 387\,072$ elements. Thus, the orbit of any state from HL under the action of the (extended) Clifford group is the union of 240 copies of HL. It was proved recently in [45,46] that this set constitutes a 3-design in $\mathcal{P}(\mathbb{C}^8)$.

It is well known that $\overline{\mathcal{C}}(8)$ is a (unique) nonsplit extension of the symplectic group Sp(6,2) by P_3 [47–50]. It means that $\overline{\mathcal{C}}(8)$ acts on P_3 by conjugation as Sp(6,2), but Sp(6,2) is not embeddable in $\overline{\mathcal{C}}(8)$. In yet other words, though the elements of $\overline{\mathcal{C}}(8)$ can be labeled by the elements of the set $P_3 \times \mathrm{Sp}(6,2)$, this group is not a semidirect product of P_3 by Sp(6,2), and, in particular, the product of two elements from $\overline{\mathcal{C}}(8)$ labeled by $(0,M_1)$ and $(0,M_2)$ for $M_1,M_2 \in \mathrm{Sp}(6,2)$ may have a nonzero first coordinate (see Theorem 2 of [51]).

Let ψ be a *fiducial* vector for HL, i.e., one of the vectors from $\mathcal{P}(\mathbb{C}^8)$ generating $HL = (P_3)\psi$. Then, it is easy to show that $\mathrm{Sym}_U\,(HL) = P_3 \rtimes (\mathrm{Sym}_U\,(HL))_\psi$, where $(\mathrm{Sym}_U\,(HL))_\psi$ is the stabilizer of ψ in $\mathrm{Sym}_U\,(HL)$. In consequence, $(\mathrm{Sym}_U\,(HL))_\psi \simeq \mathrm{Sym}_U\,(HL)/P_3$ is a subgroup of $\overline{\mathcal{C}}(8)/P_3 \simeq \mathrm{Sp}(6,2)$. Moreover, we know from Sec. 10.4 of [12] that $(\mathrm{Sym}_U\,(HL))_\psi$ has 6 048 elements. However, there is only one (up to isomorphism) subgroup of Sp(6,2) of order 6 048, namely the derived Chevalley group $G_2'(2)$ [52]. Consequently, $(\mathrm{Sym}_U\,(HL))_\psi \simeq G_2'(2)$, and so $\mathrm{Sym}_U\,(HL) \simeq P_3 \rtimes G_2'(2)$. However, in spite of the fact that $(\mathrm{Sym}_U\,(HL))_\psi \rtimes \mathbb{Z}_2 \simeq (\mathrm{Sym}\,(HL))_\psi$ and $G_2'(2) \rtimes \mathbb{Z}_2 \simeq G_2(2)$, where $G_2(2)$ is the Chevalley group of order 12 096, it is not clear whether $(\mathrm{Sym}\,(HL))_\psi \simeq G_2(2)$.

It is natural to consider normalized rank-1 POVMs as subsets of the complex projective space. It seems that the Hoggar lines are exceptional also in this context. Clearly, they form a symmetric set, as every SIC-POVM known so far does, but in fact they exhibit a higher level of symmetry. Together with the "tetrahedral" SIC-POVM in dimension two and the Hesse SIC-POVM in dimension three, they are the only SIC-POVMs that are *supersymmetric*, which means that $\mathrm{Sym}\,(HL)$ acts doubly transitively on HL (see Theorem 1 in [53]). As a consequence, one can deduce (see Corollary 1 in [27]) that they form a *highly symmetric* subset of $\mathbb{C}P^7$ in the sense of [27], which was observed by Zhu [53].

There exist other constructions of HL that were proposed by Grassl (Sec. 4.2.2 in [54]; the fact that his construction does indeed lead to the set of Hoggar lines was later noticed by Zhu [12]), Godsil and Roy [55], Jiangwei [8], and Jedwab and Wiebe [28,56,57]. We use the last of these in the present paper.

V. MAIN RESULTS

Let us recall that a *complex Hadamard matrix* $H = (h_{ij})_{i,j=0}^{d-1}$ is a $d \times d$ matrix such that $|h_{ij}|^2 = 1$ for $i,j = 0,\ldots,d-1$, and

$$HH^\dagger = d\,\mathrm{I}_d.$$

In particular, if all its entries lie in $\{-1,1\}$, then H is called a *real Hadamard matrix*. In this case

$$\sum_{l=0}^{d-1} h_{jl}^2 = d, \quad \text{for } j = 0,\ldots,d-1, \tag{2}$$

and

$$\sum_{l=0}^{d-1} h_{jl}h_{ml} = 0, \quad \text{for } j,m = 0,\ldots,d-1,\ j \neq m. \tag{3}$$

Two Hadamard matrices H and H' are called *equivalent* if there exist permutation matrices P, P' and diagonal unitary matrices D, D' such that $H' = DPHP'D'$.

Jedwab and Wiebe [28,56,57] recently proposed a simple method of constructing SIC-POVMs in certain dimensions, which employs complex Hadamard matrices. We recall it briefly below.

Let H be a complex Hadamard $d \times d$ matrix and let $v \in \mathbb{C}$. Consider the set $H(v) := \{H_{jk}(v)\}_{j,k=0}^{d-1}$ of d^2 vectors in $\mathbb{C}^d$ such that $H_{jk}(v)$ is the jth row of H with the kth coordinate multiplied by v. Denoting the canonical orthonormal basis in $\mathbb{C}^d$ by $(e_l)_{l=0}^{d-1}$ we can write $H_{jk}(v)$ as $H_{jk}(v) = \sum_{l=0}^{d-1} h_{jl}e_l + (v-1)h_{jk}e_k$. Jedwab and Wiebe proved in Theorem 1 of [28] that $H(v)$ generates a set of d^2 equiangular lines in $\mathbb{C}^d$ if and only if

(i) $d = 2$ and $v \in \{\pm(1 \pm \sqrt{3})(1 \pm i)/2\}$, or
(ii) $d = 3$ and $v \in \{0, -2, 1 \pm \sqrt{3}i\}$, or
(iii) $d = 8$, H is equivalent to a (unique up to equivalence) real Hadamard matrix and $v \in \{-1 \pm 2i\}$.

Moreover, for $d = 8$ the obtained sets of equiangular lines are the Hoggar lines. On the other hand, for $d = 2$ every complex Hadamard matrix is necessarily equivalent to a real Hadamard matrix, and all the SIC-POVMs are isomorphic to the "tetrahedral" one.

From now on, we denote the SIC-POVM corresponding to $H(v)$ by the same letter if no confusion arises. Now we can formulate the main results of the present paper:

Theorem 1. Let a complex Hadamard matrix H in dimension $d \in \{2,8\}$ and $v \in \mathbb{C}$ be such that $H(v) := \{H_{jk}(v)\}_{j,k=0}^{d-1}$ forms a set of equiangular vectors. Then the entropy of $H(v)$ is minimized by d^2 states in $H(\bar{v})$. Moreover, the minimal value of entropy is $\ln(d(d+1)/2)$.

Proof. Set $m,n = 0,\dots,d-1$. First, we show that the sequence $T_{mn} := (|H_{jk}(v) \cdot H_{mn}(\bar{v})|^2)_{j,k=0}^{d-1}$ consists of only two elements, one of which is zero. We know that there exist a real Hadamard matrix H' and diagonal unitary matrices $D = \mathrm{diag}(c_1,\dots,c_d)$ and $D' = \mathrm{diag}(c_1',\dots,c_d')$ such that $H = DH'D'$. Clearly, $(e_l')_{l=0}^{d-1}$, where $e_l' := c_l' e_l$ $(l = 0,\dots,d-1)$ is also an orthonormal basis of $\mathbb{C}^d$. Then

$$H_{jk}(v) = c_j\left(\sum_{l=0}^{d-1} h_{jl}' e_l' + (v-1) h_{jk}' e_k'\right)$$

for $j,k = 0,\dots,d-1$, and so

$$|H_{jk}(v) \cdot H_{mn}(\bar{v})| = |H_{jk}'(v) \cdot H_{mn}'(\bar{v})|$$

for $j,k,m,n = 0,\dots,d-1$. This identity reduces calculations to the real case, and so from now on we assume that H is a real Hadamard matrix.

Now, using Eqs. (2) and (3), we get

$$\begin{aligned}
&|H_{jk}(v) \cdot H_{mn}(\bar{v})|^2 \\
&= \left|\sum_{l,r=0}^{d-1} h_{jl} h_{mr} e_l \cdot e_r + \sum_{l=0}^{d-1} (v-1)(h_{jl} h_{mn} e_l \cdot e_n \right. \\
&\quad \left. + h_{jk} h_{ml} e_k \cdot e_l) + (v-1)^2 h_{jk} h_{mn} e_k \cdot e_n \right|^2 \\
&= |d\delta_{jm} + (v-1)(h_{jn} h_{mn} + h_{jk} h_{mk}) \\
&\quad + (v-1)^2 h_{jk} h_{mn} \delta_{kn}|^2.
\end{aligned}$$

In particular, for $j \neq m$ and $k \neq n$ we have

$$|H_{jk}(v) \cdot H_{mn}(\bar{v})|^2 = |(v-1)(h_{jn} h_{mn} + h_{jk} h_{mk})|^2. \tag{4}$$

It follows from Eq. (3) and from the fact that the entries of H are ± 1 that for all $m,n,j = 0,\dots,d-1$ and $j \neq m$ there exist exactly $d/2$ such $k = 0,\dots,d-1$ that the above expression is equal to zero. Otherwise, it is $|2v-2|^2$.

For $j \neq m$ and $k = n$ we get

$$|H_{jk}(v) \cdot H_{mk}(\bar{v})|^2 = |v^2 - 1|^2;$$

on the other hand, for $j = m$ and $k \neq n$ we obtain

$$|H_{jk}(v) \cdot H_{jn}(\bar{v})|^2 = |d + 2v - 2|^2,$$

and finally, for $j = m$ and $k = n$ we have

$$|H_{jk}(v) \cdot H_{jk}(\bar{v})|^2 = |d + v^2 - 1|^2.$$

Now, straightforward calculations show that for the values of v obtained by Jedwab and Wiebe [28] all the $d(d+1)/2$ nonzero members of the sequence T_{mn} are equal and depend only on d and v. This, in turn, implies that T_{mn} attains value zero with multiplicity $(d-1)d/2$.

Let us now consider the premeasurement state generated by $H_{mn}(\bar{v})$ for $m,n = 0,\dots,d-1$, and the SIC-POVM $H(v)$. In this case, as has just been shown, the distribution of measurement outcomes provides us with $d(d+1)/2$ probabilities equal to $2/[d(d+1)]$ and $(d-1)d/2$ equal to zero. According to the result discussed in Sec. III, the state generated by $H_{mn}(\bar{v})$ must be a minimizer for the entropy of $H(v)$ and the minimal value is equal to $\ln(d(d+1)/2)$. ■

Theorem 2. Under the assumptions of Theorem 1, the informational power of $H(v)$ is equal to $\ln(2d/(d+1))$, and the states generated by the vectors in $H(\bar{v})$ constitute an equiprobable maximally informative ensemble. In particular, the informational power of Hoggar lines is $2\ln(4/3)$.

Proof. Since $\mathrm{Sym}(H(v))$ acts irreducibly on $\mathcal{P}(\mathbb{C}^d)$, the equality in Eq. (1) holds for $\Pi = H(v)$. Hence, applying Eq. (1) and Theorem 1, we get

$$W(\Pi) = \ln(d^2) - \ln(d(d+1)/2) = \ln(2d/(d+1)).$$

Then d^2 equiprobable states corresponding to the vectors from $H(\bar{v})$ form a maximally informative ensemble. ■

VI. MUCH ADO ABOUT ZEROS

In the above reasoning the zeros of the probability distribution of measurement outcomes play a key role. For the Hoggar lines we already know that for the premeasurement state of the system being the entropy minimizer, their number equals 28, which is the maximum possible number of zero probabilities; see [3]. Let us now have a closer look at the localization of these 28 zeros for 64 minimizers described by Theorem 1.

From now on we label the elements of the Hoggar lines SIC-POVM $H(v)$ by the elements of $\Sigma := \mathbb{Z}_2^3 \otimes \mathbb{Z}_2^3$, the translation group of the six-dimensional affine space over GF(2), isomorphic to P_3 acting regularly on $H(v)$. Moreover, we assume for definiteness that H is the (real) Sylvester-Hadamard matrix H_3 considered, e.g., in [28], writing the indices in the binary expansion as elements of $\mathbb{Z}_2^3$. In this case we have $h_{\iota\kappa} = (-1)^{\iota_1\kappa_1+\iota_2\kappa_2+\iota_3\kappa_3}$ for $\iota,\kappa \in \mathbb{Z}_2^3$. Moreover, the standard representation of the three-qubit Pauli group, constructed from the Pauli matrices σ_X and σ_Z, acts (up to a phase) on vectors in $H(v)$ and $H(\bar{v})$ in the following way:

$$\left(\sigma_Z^{\alpha_1}\sigma_X^{\beta_1} \otimes \sigma_Z^{\alpha_2}\sigma_X^{\beta_2} \otimes \sigma_Z^{\alpha_3}\sigma_X^{\beta_3}\right) H_{\iota\kappa}(w) = H_{\iota+\alpha,\kappa+\beta}(w)$$

for $\iota,\kappa,\alpha,\beta \in \mathbb{Z}_2^3, w = v,\bar{v}$. Consider now the blocks

$$B_{\mu\nu} := \left\{(\iota,\kappa) : H_{\iota\kappa}(v) \cdot H_{\mu\nu}(\bar{v}) = 0, \iota,\kappa \in \mathbb{Z}_2^3\right\},$$

of zeros of $T_{\mu\nu}$ for $\mu,\nu \in \mathbb{Z}_2^3$, where $T_{\mu\nu}$ is as in the proof of Theorem 1. It follows from Eq. (4) that $(\iota,\kappa) \in B_{\mu\nu}$ if and only if $\iota \neq \mu, \kappa \neq \nu$, and $h_{\mu\nu}h_{\iota\nu} + h_{\mu\kappa}h_{\iota\kappa} = 0$, or equivalently $h_{\mu+\iota,\nu+\kappa} = -1$, for $\iota,\kappa \in \mathbb{Z}_2^3$. Hence $B_{00} = \{(\iota,\kappa) : h_{\iota\kappa} = -1, \iota,\kappa \in \mathbb{Z}_2^3\}$ and $B_{\mu\nu} = B_{00} + (\mu,\nu)$ for $\mu,\nu \in \mathbb{Z}_2^3$. It is easy to show that $\mathscr{B}_8 := \{B_{\mu\nu}\}_{\mu,\nu\in\mathbb{Z}_2^3} \subset \Sigma$ constitutes a *symmetric* (*Menon*) (64,28,12)-*design*; see [58] for terminology from design theory. Moreover, this design is the development of the respective *difference set* in Σ. More precisely, one can show that $\mathscr{B}_8$ is the so-called *symplectic design* $\mathscr{S}^{-1}(6)$ analyzed by Kantor in [59]. He proved that Aut $[\mathscr{S}^{-1}(6)]$, the automorphism group of $\mathscr{S}^{-1}(6)$, is a semidirect product of Σ by the symplectic group Sp(6,2), i.e., the group of linear transformations of the vector space $\mathbb{Z}_2^6 \simeq \Sigma$ over GF (2) preserving the natural symplectic form. More precisely, for all $(\iota,\kappa) \in \Sigma$ and $M \in \mathrm{Sp}(6,2)$ the respective affine transformation sends $B_{\mu\nu}$ onto $B_{M(\mu,\nu)+(\iota,\kappa)}$ for all $\mu,\nu \in \mathbb{Z}_2^3$. Moreover, Aut $(\mathscr{S}^{-1}(6))$ acts 2-transitively on blocks [59].

VII. TWIN SETS OF HOGGAR LINES

Now, let us have a closer look at the set $H(\bar{v})$, all of whose elements are minimizers for the entropy of $H(v)$, and form a maximally informative ensemble for this measurement. It follows from Theorem 1 (this paper) and Theorem 1 in [28] that $H(\bar{v})$ is also the "tetrahedral" POVM for $d = 2$, and the set of Hoggar lines for $d = 8$. The question arises of how these two subsets of $\mathcal{P}(\mathbb{C}^d)$, $H(v)$ and $H(\bar{v})$, are related to one another. Let $C : \mathbb{C}^d \to \mathbb{C}^d$ be a (*complex*) *conjugation* with respect to the basis $(e_l')_{l=0}^{d-1}$ from the proof of Theorem 1, i.e., an antiunitary involutive map keeping the basis invariant [60], given by $C(\sum_{l=0}^{d-1} x_l e_l') := \sum_{l=0}^{d-1} \bar{x}_l e_l'$ for $(x_l)_{l=0}^{d-1} \in \mathbb{C}^d$. Then $H(\bar{v})$ is the image of $H(v)$ under the collineation generated by C; more precisely, $H_{jk}(\bar{v}) = C(H_{jk}(v))$ for $j,k = 0,\ldots,d-1$.

To express the relationship between $H(v)$ and $H(\bar{v})$ more geometrically, we can use the generalized Bloch representation. For $d = 2$, these SIC-POVMs are represented on the Bloch sphere as two dual regular tetrahedra that together form a stellated octahedron, also known as *stella octangula*. For $d = 8$ we get in the generalized Bloch representation two regular 63-dimensional simplices inscribed in the unit sphere in a 63-dimensional real vector space, where one is the image of the other under a reflection through a 35-dimensional linear subspace. It is so, because in the generalized Bloch representation of quantum states as elements of the unit sphere of the real $(d^2 - 1)$-dimensional vector space of traceless Hermitian $d \times d$ matrices, a conjugation map acting on $\mathbb{C}^d$ is transformed into a transpose operation (both defined in the same basis); see, e.g., p. 4 of [61]. Under this operation only traceless symmetric real matrices are invariant, and they form a $[(d + 2)(d - 1)/2]$-dimensional vector subspace.

Moreover, it turns out that for $d = 8$ the sets $H(v)$ and $H(\bar{v})$ correspond to "twin" sets of Hoggar lines considered in Sec. 2.3 of [53]. Let ψ be a fiducial vector for some HL. Zhu showed that there is an order-seven unitary U_7 in $(\mathrm{Sym}\,(HL))_\psi$ with six one- and one two-dimensional eigenspaces, such that the latter contains both ψ and its twin vector, ψ', which also generates (another) set of Hoggar lines HL', lying on the same orbit under action of the Clifford group. To be more specific, assume again that $H = H_3$. Let us consider a fiducial vector $\psi := \frac{1}{\sqrt{6}}(-i,-1,0,0,-1+i,0,1,1)^{\mathrm{T}}$ and its twin $\psi' := \frac{1}{\sqrt{6}}(1+i,0,-1,1,-i,-1,0,0)^{\mathrm{T}}$ given by Eqs. (14) and (3) in [53]. Then, all four sets of Hoggar lines, $H(v)$, $H(\bar{v})$, and those generated by ψ and ψ', are covariant with respect to the standard representation of the three-qubit Pauli group. Let U denote a Clifford unitary for this group given by (p. 28 of [28])

$$U := \frac{1}{2}\begin{pmatrix} 0 & 0 & i & -1 & 0 & 0 & 1 & i \\ 0 & 0 & -1 & i & 0 & 0 & i & 1 \\ -1 & i & 0 & 0 & -i & -1 & 0 & 0 \\ -i & 1 & 0 & 0 & 1 & i & 0 & 0 \\ 0 & 0 & -i & 1 & 0 & 0 & 1 & i \\ 0 & 0 & 1 & -i & 0 & 0 & i & 1 \\ 1 & -i & 0 & 0 & -i & -1 & 0 & 0 \\ i & -1 & 0 & 0 & 1 & i & 0 & 0 \end{pmatrix}.$$

Now, observe that, up to a normalization factor, $U\psi = H_{(0,0,0)(0,1,1)}(v)$ and $U\psi' = H_{(1,0,1)(0,0,0)}(\bar{v})$, and they are indeed fiducial vectors, respectively, for $H(v)$ and $H(\bar{v})$, lying in the same two-dimensional eigenspace of an order-seven unitary $UU_7U^\dagger$.

Finally, note that the symmetry groups of both Hoggar SIC-POVMs, $H(v)$ and $H(\bar{v})$, are identical. It follows from the fact that the symmetry groups of the "twin" sets of Hoggar lines HL and HL' described above are the same. Indeed, these symmetry groups are generated by the same representation of the three-qubit Pauli group and, respectively, the stabilizers of ψ and ψ'. Thus, it suffices to show that the stabilizer of ψ' is contained in the symmetry group of HL. The stabilizer has two generators: U_7, which stabilizes both fiducials, and U_{12}, an order-12 unitary defined in Sec. 10.4 of [12]. By straightforward calculation, we get that U_{12} permutes the elements of HL and so belongs to its symmetry group. The situation is similar for two dual "tetrahedral" POVMs in $d = 2$ sharing also the same symmetry group.

ACKNOWLEDGMENTS

We are thankful to Christopher Fuchs for helpful remarks. Financial support by the NCN Grant No. 2015/18/A/ST2/00274 is gratefully acknowledged.

[1] C. A. Fuchs, arXiv:1003.5209 [quant-ph].
[2] C. M. Caves, C. A. Fuchs, and R. Schack, J. Math. Phys. **43**, 4537 (2002).
[3] D. M. Appleby, Å. Ericsson, and C. A. Fuchs, Found. Phys. **41**, 564 (2011).
[4] B. C. Stacey, Mathematics **4**, 36 (2016).
[5] J. M. Renes, Quantum Inf. Comput. **5**, 81 (2005).
[6] A. J. Scott, J. Phys. A **39**, 13507 (2006).
[7] H. Zhu and B.-G. Englert, Phys. Rev. A **84**, 022327 (2011).
[8] S. Jiangwei, Ph.D. thesis, National University of Singapore, 2013.
[9] N. Bent, H. Qassim, A. A. Tahir, D. Sych, G. Leuchs, L. L. Sánchez-Soto, E. Karimi, and R. W. Boyd, Phys. Rev. X **5**, 041006 (2015).
[10] O. Oreshkov, J. Calsamiglia, R. Muñoz Tapia, and E. Bagan, New J. Phys. **13**, 073032 (2011).
[11] B. Chen, T. Li, and S.-M. Fei, Quantum Inf. Process. **14**, 2281 (2015).

[12] H. Zhu, Ph.D. thesis, National University of Singapore, 2012.
[13] D. M. Appleby, H. B. Dang, and C. A. Fuchs, Entropy **16**, 1484 (2014).
[14] T.-Y. Chien, Ph.D. thesis, University of Auckland, 2015.
[15] M. Appleby, S. Flammia, G. McConnell, and J. Yard, arXiv:1604.06098.
[16] D. M. Appleby, C. A. Fuchs, and H. Zhu, Quantum Inf. Comput. **15**, 61 (2015).
[17] J. Mann, Rose-Hulman Undergraduate Math. J. **14**, 101 (2013).
[18] L. P. Hughston and S. M. Salamon, Adv. Math. **286**, 1017 (2016).
[19] S. G. Hoggar, in *The Geometric Vein, Coxeter Festschrift*, edited by C. Davis, B. Grnbaum, and F. A. Sherk (Springer-Verlag, New York, 1981), pp. 219–230.
[20] M. Dall'Arno, G. M. D'Ariano, and M. F. Sacchi, in *Eleventh International Conference on Quantum Communication, Measurement and Computation (QCMC)*, edited by H.-J. Schmiedmayer and P. Walther, AIP Conf. Proc. 1633 (AIP Publishing, Melville, NY, 2014), pp. 150–152.
[21] M. Dall'Arno, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **83**, 062304 (2011).
[22] A. S. Holevo, Probl. Inf. Transm. (Engl. Transl.) **48**, 1 (2012).
[23] M. Dall'Arno, F. Buscemi, and M. Ozawa, J. Phys. A **47**, 235302 (2014).
[24] M. Dall'Arno, Phys. Rev. A **90**, 052311 (2014).
[25] A. Szymusiak, J. Phys. A **47**, 445301 (2014).
[26] M. Dall'Arno, Phys. Rev. A **92**, 012328 (2015).
[27] W. Słomczyński and A. Szymusiak, Quantum Inf. Process. **15**, 565 (2016).
[28] J. Jedwab and A. Wiebe, in *Algebraic Design Theory and Hadamard Matrices*, edited by C. Colbourn (Springer-Verlag, New York, 2015), pp. 159–169.
[29] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, J. Math. Phys. **45**, 2171 (2004).
[30] A. Szymusiak (unpublished).
[31] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).
[32] E. B. Davies, IEEE Trans. Inf. Theory **24**, 596 (1978).
[33] M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki, and O. Hirota, Phys. Rev. A **59**, 3325 (1999).
[34] P. W. Shor, J. Math. Phys. **43**, 4334 (2002).
[35] A. S. Holevo, Int. J. Quantum Inf. **3**, 41 (2005).
[36] F. E. Schroeck, Jr., J. Math. Phys. **30**, 2078 (1989).
[37] J. Sánchez-Ruiz, Phys. Lett. A **201**, 125 (1995).
[38] G. C. Ghirardi, L. Marinatto, and R. Romano, Phys. Lett. A **317**, 32 (2003).
[39] D. Ellerman, Int. J. Semant. Comput. **11**, 121 (2013).
[40] P. Harremoës and F. Topsøe, IEEE Trans. Inf. Theory **47**, 2944 (2001).
[41] K. Życzkowski, Open Syst. Inf. Dyn. **10**, 297 (2003).
[42] S. G. Hoggar, Math. Scand. **43**, 241 (1978).
[43] S. G. Hoggar, Geom. Dedicata **69**, 287 (1998).
[44] G. Zauner, Ph.D. thesis, Universität Wien, 1999.
[45] Z. Webb, arXiv:1510.02769.
[46] H. Zhu, arXiv:1510.02619.
[47] B. Bolt, T. G. Room, and G. E. Wall, J. Aust. Math. Soc. **2**, 60 (1961).
[48] B. Bolt, T. G. Room, and G. E. Wall, J. Aust. Math. Soc. **2**, 80 (1961).
[49] U. Dempwolff, Illinois J. Math. **18**, 451 (1974).
[50] A. B. M. Basheer and J. Moori, Bull. Iran. Math. Soc. **39**, 1189 (2013).
[51] J. Dehaene and B. De Moor, Phys. Rev. A **68**, 042318 (2003).
[52] T. Connor and D. Leemans, arXiv:1306.4820.
[53] H. Zhu, Ann. Phys. (NY) **362**, 311 (2015).
[54] M. Grassl, Electron. Notes Discrete Math. **20**, 151 (2005).
[55] C. Godsil and A. Roy, Eur. J. Combin. **30**, 246 (2009).
[56] A. D. Wiebe, Ph.D. thesis, Simon Fraser University, 2013.
[57] J. Jedwab and A. Wiebe, Des. Codes Cryptogr. **80**, 73 (2016).
[58] E. H. Moore and H. S. Pollatsek, *Difference Sets: Connecting Algebra, Combinatorics, and Geometry* (American Mathematical Society, Providence, RI, 2013).
[59] W. M. Kantor, J. Algebra **33**, 43 (1975).
[60] S. R. Garcia, E. Prodan, and M. Putinar, J. Phys. A **47**, 353001 (2014).
[61] J. M. Leinaas, J. Myrheim, and E. Ovrum, Phys. Rev. A **74**, 012313 (2006).