Jagiellonian University
Faculty of Mathematics and Computer Science
Institute of Mathematics

Minimization of the entropy of measurement for symmetric POVMs and their informational power

Anna Szymusiak

PhD Thesis written under supervision
of dr hab. Wojciech Słomczyński, prof. UJ

Kraków, 2014

Acknowledgments

I wish to start with expressing my gratitude to my supervisor Professor Wojciech Słomczyński. It was he, who introduced me into the quantum information theory and was not discouraged by my initial ignorance in the topic. Due to his inquiries I made my mind to apply to the PhD studies. He was a great guide on the roads of academic life and I could learn a lot from him about the methodology of the scientific work. I have always admired his spirit of inquiry, wide interests and extensive knowledge. I want to thank him for the immense amount of time during these six years (including tutoring during my master studies), for the patience, long and fruitful discussions and an unceasing belief in my finishing the thesis in four years.

Many thanks to Professor Karol Życzkowski who leads with Professor Wojciech Słomczyński the weekly seminar on chaos and quantum information. My knowledge and understanding of the quantum information theory has significantly increased by the possibility of listening to the seminar talks, many a time given by the invited world renowned specialists. In this place I could not afford not to mention his insightful comments and his special ability to ask the most accurate questions and answer them in the most intuitive way.

My real math adventure would probably not take place unless I had chosen the theoretical mathematics for my specialization. I owe to Professor Halszka Tutaj-Gasińska and Doctor Joanna Orewczyk the fact I did not give up the idea of attending the classes for theoreticians and in consequence could benefit from taking the more advanced and challenging courses.

Last but not least I want to thank my dear Family for their love and support during whole my life and especially during the last years. I am extremely grateful to my Parents for the freedom they gave all of us in choosing the field of study, asking us just one question, whether would we be happy with our choice, as well as for their willingness to do everything they could to enable our education. Many thanks to my elder brothers, Paweł and Michał, who used to attribute my interest in mathematics to their way of babysitting me by giving me some counting tasks (so I would not interrupt them). Well done, guys!

Contents

List of Figures

List of Tables

List of frequently used symbols

$\mathcal{L}(\mathcal{H})$, $\mathcal{L}(\mathbb{C}^d)$	(bounded) linear operators on $\mathcal{H}$ ($\mathbb{C}^d$)
$\mathcal{L}_s(\mathcal{H})$, $\mathcal{L}_s(\mathbb{C}^d)$	(bounded) self-adjoint operators
$\mathcal{L}_s^+(\mathcal{H})$, $\mathcal{L}_s^+(\mathbb{C}^d)$	(bounded) self-adjoint positive-semidefinite operators
$\mathcal{L}_s^0(\mathcal{H})$, $\mathcal{L}_s^0(\mathbb{C}^d)$	(bounded) self-adjoint traceless operators
$\mathbb{I}$	identity operator (on $\mathcal{H}$)
$\mathcal{P}(\mathcal{H})$, $\mathcal{P}(\mathbb{C}^d)$	set of pure states ($\rho \in \mathcal{L}(\mathcal{H}), \rho \geq 0, \rho^2 = \rho$, $\mathrm{Tr}(\rho) = 1$)
$\mathcal{S}(\mathcal{H})$, $\mathcal{P}(\mathbb{C}^d)$	set of (mixed) states ($\rho \in \mathcal{L}(\mathcal{H}), \rho \geq 0$ and $\mathrm{Tr}(\rho) = 1$)
D_{FS}	Fubini-Study metric on $\mathbb{CP}^{d-1}$ or $\mathcal{P}(\mathbb{C}^d)$
m_{FS}	unique unitarily invariant measure on $\mathbb{CP}^{d-1}$ or $\mathcal{P}(\mathbb{C}^d)$
$\langle\langle \cdot, - \rangle\rangle_{HS}$	Hilbert-Schmidt inner product
$b(\rho)$, $\vec{b}_\rho$	Bloch vectors corresponding to state ρ in $\mathcal{L}_s^0(\mathbb{C}^d)$ and $\mathbb{R}^{d^2-1}$, respectively
$B(d)$	set of normalized Bloch vectors corresponding to pure states in $S^{d^2-2} \subset \mathbb{R}^{d^2-1}$
$\mathrm{U}(\mathcal{H})$ ($\mathrm{U}(d)$)	unitary group
$\mathrm{UA}(\mathcal{H})$ ($\mathrm{UA}(d)$)	unitary-antiunitary group
$\mathrm{PU}(\mathcal{H})$ ($\mathrm{PU}(d)$)	projective unitary group
$\mathrm{PUA}(\mathcal{H})$ ($\mathrm{PUA}(d)$)	projective unitary-antiunitary group
σ_U	isometry of $(\mathcal{P}(\mathcal{H}), D_{FS})$ given by $\rho \mapsto U\rho U^*$ for $U \in \mathrm{UA}(\mathcal{H})$
η	Shannon entropy function
$H(\cdot, \Pi)$, $\widetilde{H}(\cdot, \Pi)$	entropy and relative (with respect to the uniform distribution) entropy of POVM Π
H_B, $\widetilde{H}_B$	entropy and relative entropy of POVM redefined to be functions of Bloch vectors
H_α, R_α	Tsallis α-entropy, Rényi α-entropy
$I(V, \Pi)$	mutual information between ensemble of initial states V and POVM Π
$W(\Pi)$	informational power of Π
Δ_k	probability simplex
$\mathrm{Sym}(S)$	group of symmetries of S
Gx	orbit of x under action of group G
G_x	stabilizer of x
Σ_x	orbit stratum of x

$N_H(G)$	normalizer of H in G
D_{nh}, T_d, O_h, I_h	prismatic, full tetrahedral, full octahedral, full icosahedral group
τ	golden ratio
H_d	finite Weyl-Heisenberg group
$D_{\mathbf{p}}$	Weyl matrix
$\mathrm{C}(d)$, $\mathrm{EC}(d)$	Clifford group, extended Clifford group (normalizers of H_d in $\mathrm{U}(d)$ and $\mathrm{UA}(d)$, respectively)
$\mathrm{ESL}(2, \mathbb{Z}_d)$	extended special linear group of all 2×2 matrices over $\mathbb{Z}_d$ with determinant ± 1
$\mathrm{I}(d)$	group of unitary multiples of $\mathbb{I}$ (on $\mathbb{C}^d$)
$\mathcal{I}$	identity matrix in $\mathrm{ESL}(2, \mathbb{Z}_d)$
$\mathcal{Z}$	Zauner matrix $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ in $\mathrm{ESL}(2, \mathbb{Z}_d)$
$U_{(\mathcal{F},\mathbf{r})}$	canonical order 3 unitary corresponding to $(\mathcal{F}, \mathbf{r})$

CHAPTER 0

Introduction

'I discard all hope of predicting hitherto unpredictable quantities, such as my graduation.' – Werner Heisenberg

(Jorge Cham, *PhD Comics: Quantum Gradnamics, pt. 2 of 3*)

0.1. The problem statement. Motivation.

Uncertainty is an intrinsic property of quantum physics: typically, a measurement of an observable can yield different results for two identically prepared states. This indeterminacy can be studied by considering the probability distribution of measurement outcomes given by the Born rule, and quantized by a number that characterizes the randomness of this distribution. The Shannon entropy is the most natural tool for this purpose. Obviously, the value of this quantity is determined by the choice of the initial state of the system before the measurement. When the number of possible measurement outcomes is finite and equals k, it varies from 0, if the measurement outcome is determined, to $\ln k$, if all outcomes are equiprobable. If the measured observable is represented by a normalized rank-1 positive-operator valued measure (POVM) on a d-dimensional complex Hilbert space, then the upper bound is achieved for the maximally mixed state $\mathbb{I}/d$. On the other hand, the Shannon entropy of measurement cannot be 0 unless the POVM is a projection valued measure (PVM) representing projection (Lüders-von Neumann) measurement with $k = d$, since it is bounded from below by $\ln(d/k)$. Thus in the general case the following questions arise: how to choose the input state to minimize the uncertainty of the measurement outcomes, and what is the minimum value of the Shannon entropy for the distribution of measurement results in this case? In the present paper we call this number the *entropy of measurement*.

The entropy of measurement has been widely studied by many authors since the 1960s [**162**], also in the context of entropic uncertainty principles [**59**], as well as in quantum information theory under the name of *minimum output entropy of a quantum-classical channel* [**143**]. Subtracting this quantity from $\ln k$, we get the *relative entropy of measurement* (with respect to the uniform distribution), which may vary from 0 to $\ln d$. In consequence, the optimization problem now reduces to finding its maximum value. Either way, we are looking for the 'least quantum' or 'most classical' states in the sense that the measurement of the system prepared in such a state gives the most defined results. Because of concavity of the entropy of measurement as a function of state, we know that the optimal states must be pure.

Like many other optimization problems where the Shannon function $\eta(x) = -x \ln x$ is involved, the minimization of the entropy of measurement seems to be too difficult to be solved analytically in the general case. In fact, analytical solutions have been found so far only for a few two-dimensional (qubit) cases, where the Bloch vectors of POVM elements constitute an n-gon [**137, 70, 11**], a tetrahedron [**117**] or an octahedron [**132, 45**]. All these POVMs are symmetric (group covariant), but, as we shall see, symmetry alone is not enough to solve the problem analytically. However, for symmetric rank-1 POVMs the relative entropy of measurement gains an additional interpretation. It follows from [**117**], that it is equal to the *informational power of measurement* [**11, 12**], viz., the *classical capacity of a quantum-classical channel* generated by the POVM [**90**]. To distinguish the class of measurements for which the entropy minimization problem is feasible, we define *highly symmetric* (*HS*) normalized rank-1 POVMs as the symmetric subsets of the state space without non-trivial factors of an equal or higher symmetry.

The problem considered in the thesis has a well-known continuous counterpart: the minimization of the Wehrl entropy over all pure states, see Sect. 3.3, where the (approximate) quantum measurement is described by an infinite family of group coherent states generated by a unitary and irreducible action of a linear group on a highly symmetric fiducial vector representing the vacuum. More than thirty years ago Lieb [**105**], and quite recently Lieb & Solovej [**106**] proved for harmonic oscillator and spin coherent states, respectively, that the minimum value of the Wehrl entropy is attained, when the state before the measurement is also a coherent state. Surprisingly, an analogous theorem need not be true in the discrete case, since the entropy of measurement need not be minimal for the states constituting the POVM, and in fact for SIC-POVMs quite the opposite is true: the entropy for these states is maximal, see Sect. 4.5. This discrepancy requires further study.

The minimization of the entropy of measurement is also closely related to entropic uncertainty principles [**161**]. Indeed, every such principle leads to a lower bound for the entropy of some measurement, and conversely, such bounds may yield new uncertainty principles for single or multiple measurements. Moreover, in Sect. 3.5 we reveal the connection between the entropy of measurement and the quantum dynamical entropy with respect to this measurement [**145**], the quantity introduced independently by different authors to analyse the results of consecutive quantum measurements interwind with a given unitary evolution.

0.2. Results and methods

In dimension two, we first classify all HS-POVMs, proving that their Bloch sphere representations must be either one of the five Platonic solids or the two quasiregular Archimedean solids (the cuboctahedron and icosidodecahedron), or belong to an infinite series of regular polygons. For such POVMs we show that their *entropy is minimal (and so the relative entropy is maximal), if and only if the input state is orthogonal to one of the states constituting a POVM.* We present a unified proof of this fact for all eight cases, and for five of them (the cube, icosahedron, dodecahedron, cuboctahedron and icosidodecahedron) the result seems to be new.

Another class of quantum measurements that will be of our particular interest are *symmetric informationally complete* POVMs (SIC-POVMs in brief) that correspond to the set of d^2 equiangular directions in $\mathbb{C}^d$. Their existence in every dimension remains an open problem. Nevertheless, some conjectures about their algebraic structure hold true for known examples in lower dimensions, thus we are equipped with tools that appear to be useful while solving the entropy minimization problem. In dimension three we claim that *the entropy of a SIC-POVM is minimal, if and only if the input state is orthogonal to one of the three subspaces spanned by triples of linearly dependent vectors constituting the SIC-POVM.* We give also an algebraic characterization of some of these minimizers and give an example where these two characterizations are not equivalent.

While we know that it suffices to search the global minimizers of the entropy among the pure states, it is natural to ask, how badly can we choose taking initially *any* pure state. In other words, it corresponds to the question, which pure state is the 'most quantum' in the sense of the most random results of a measurement performed on the system prepared in this particular state. It turns out that in the case of rank-1 normalized POVMs the pure states of maximal uncertainty of the measurement outcomes cannot appear if the measurement is informationally complete. Additionally, in dimension two the converse of this statement holds true. Moreover, we show that for SIC-POVMs in any dimension the states of maximum entropy correspond exactly to the normalized elements of the measurement itself. Finally we give a solution for informationally complete HS-POVMs in dimension two.

The general idea of solving both the minimization and maximization problem for the Shannon entropy of quantum measurement is basically the same in every case presented: to simplify the problem by simplifying the function involved. It can be done by using the Hermite interpolation in such a way that the resulting polynomial function interpolates the entropy function from below (above) and agrees with the entropy exactly in the points supposed to be the global minimizers (maximizers). These points are in most cases found by using the Michel theory of critical orbits of group invariant functions. The complexity of the minimization (maximization) problem for the interpolating polynomial function is reduced by expressing them in terms of invariant polynomials. This method can be generalized both to larger dimensions, and to other functions with similar properties as the Shannon entropy function, such as power functions leading to the Rényi entropy [**127**] or its variant, the Tsallis-Havrda-Charvát entropy [**49**], and even more general 'information functionals' studied in the same context in [**35**]. Let us emphasize that the commonly used majorization method cannot be generally applied in the considered cases.

0.3. The outline of the thesis

The thesis is organized as follows. The first chapter is devoted to the mathematical description of quantum theory. Firstly, we introduce the bra-ket notation, commonly used in the quantum community, but not so well known by mathematicians. Next, we provide the mathematical framework for the basic concepts of the theory, as quantum states and quantum measurements. Finally, the Bloch representation of the quantum states and rank-1 normalized measurements is described in details.

The second chapter starts with a brief introduction to the general concept of symmetry, including definitions of symmetric, resolving and highly symmetric sets in metric space. Then the notions of symmetric and highly symmetric quantum measurements are provided with their relation to the group-covariant measurements. In the same section the informationally complete and symmetric informationally complete POVMs are introduced. Next a complete characterization of highly symmetric POVMs in dimension two, based on the well-known classification of the finite subgroups of the 3-dimensional orthogonal group, is given. Finally, we gather some useful facts concerning the Weyl-Heisenberg SIC-POVMs.

In the third chapter we introduce the notion of the Shannon entropy of quantum measurement as a measure of uncertainty of the measurement outcomes. In this place we state the main problem of minimization of this quantity and relate it to the problem of maximization of the mutual information. In the following sections we briefly summarize the connections with the Wehrl entropy and the Lieb-Solovej theorem, the entropic uncertainty relations, and the quantum dynamical entropy.

The fourth chapter contains the original author's results. At the beginning, the general methods and tools used in proofs are described in details, including the Michel theory of critical orbits of group invariant functions, the minimization method based on the Hermite interpolation, the group invariant polynomials and the majorization technique. In the second section we provide a characterization of the critical points of the entropy of highly symmetric POVMs in dimension two which arise directly from the group-invariance. The third section contains the main result concerning HS-POVMs in dimension two, i.e. the proof that the local minimizers described in the previous section are indeed the global ones. In the fourth section we give a characterization of global minimizers of the entropy of SIC-POVMs in dimension three in both geometric and algebraic terms. Next we state the problem of maximizing entropy over pure states, indicating its non-triviality if the POVM is informationally complete. We give here exact solutions for SIC-POVMs in any dimension and for informationally complete HS-POVMs in dimension two. The last but one section contains discussion of possible alternative proofs for some cases. Finally, we refer to the informational power of measurement and calculate the mean value of relative entropy.

The vast content of this thesis is taken from the manuscripts [**148**] (in particular, the results from Sects. 4.2, 4.3 and 4.7), written in collaboration with my supervisor, and [**152**] (Sect. 4.4), the author's own work. At the moment of submitting this thesis the first paper is awaiting the review, and the second has received two positive reviews from J. Phys. A. The content of Sects. 4.5 and 4.6 has not been published yet even as a preprint.

CHAPTER 1

Mathematical framework of quantum mechanics

> 'So what kind of genius are you, anyway? (...) What are you genius at?'
> 'Quantum mechanics.'
> 'Yeah, but what field? Like, music?'
>
> (Woody Allen, *Whatever works*)

In this chapter we provide the basic concepts of quantum mechanics formulated in the mathematical language. In general approach, quantum theory is expressed in terms of separable Hilbert spaces and operator theory. However, since we are interested in the topics of quantum information theory rather than quantum mechanics in general, we focus on the finite-dimensional case.

1.1. Bra-ket notation

Let $\mathcal{H}$ be a separable complex Hilbert space. A vector $\psi \in \mathcal{H}$ is denoted by $|\psi\rangle$ (we read *ket psi*), while its dual by the Riesz representation theorem from $\mathcal{H}^*$ is denoted by $\langle\psi|$ (we read *bra psi*). Thus by $\langle\psi|\phi\rangle$ we mean the inner product of vectors ϕ and ψ (note that in this notation antilinearity is with respect to the first variable). We can also write $|\psi\rangle\langle\phi|$ to denote the operator $\{\gamma \mapsto \langle\gamma, \phi\rangle\psi | \gamma \in \mathcal{H}\} \in \mathcal{L}(\mathcal{H})$. In particular, $|\psi\rangle\langle\psi|$ is a projection onto a subspace generated by ψ and it is an orthogonal projection if $\|\psi\| = 1$. Some other useful properties are:

- $(|\psi\rangle\langle\phi|)^* = |\phi\rangle\langle\psi|$,
- $\mathrm{Tr}(|\psi\rangle\langle\phi|) = \langle\phi|\psi\rangle$.

The bra-ket notation has been introduced by Dirac in 1939 [**62**]. The origins of the names 'bra' and 'ket' are quite intuitive. Dirac came with an idea that since the inner product is written with (angle) brackets then if we call the left partial expression 'bra' and the right one 'ket' we obtain as a product 'bra-ket'. The meaningful difference with the standard mathematical notation comes from the fact that both bras and kets are proper mathematical objects.

1.2. Quantum states and measurements

The mathematical formulation of quantum mechanics is summarized in the *postulates of quantum mechanics*. Here we present the framework necessary in our thesis. With any quantum physical system one can associate as a state space a complex separable Hilbert space $\mathcal{H}$ (in fact, in quantum information theory we consider $\mathcal{H}$ of finite dimension, thus later on we assume that $\mathcal{H} = \mathbb{C}^d$). The *pure states* of the system are represented by the unit vectors in $\mathcal{H}$. Two states are not distinguishable if they differ by a unit factor, thus the states are fully characterized by the rays in $\mathcal{H}$, i.e. the elements of the complex projective space $\mathbb{P}\mathcal{H} = \mathbb{CP}^{d-1}$. Moreover, $\mathbb{P}\mathcal{H}$ can be identified with the set $\mathcal{P}(\mathcal{H})$ of one-dimensional orthogonal projections via the map $\mathbb{P}\mathcal{H} \ni [\psi] \mapsto \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle} \in \mathcal{P}(\mathcal{H})$. To avoid the potential misunderstanding to which mathematical object (vector, ray or operator) we refer, we set the following definition:

Definition 1.1. By a *pure state* of a quantum system we mean any trace class operator $\rho \in \mathcal{L}(\mathcal{H})$ such that $\rho \geq 0$, $\rho^2 = \rho$ and $\mathrm{Tr}(\rho) = 1$.

Definition 1.2. The set of *mixed states* of a quantum system is given by $\mathcal{S}(\mathcal{H}) = \{\rho \in \mathcal{L}(\mathcal{H}) | \rho \geq 0, \mathrm{Tr}(\rho) = 1\}$.

Obviously, any convex combination of pure states is positive-semidefinite and of trace one. On the other hand, any such operator can be written as a convex combination of the orthogonal projections onto its eigenvectors with corresponding eigenvalues as coefficients. Thus we obtain

Fact 1.1. Mixed states of a quantum system are convex combinations of pure states.

The coefficients in the convex combination can be interpreted as the probabilities of the corresponding pure states. Thus, the elements of $\mathcal{S}(\mathcal{H})$ are also called *density operators*. Note, however, that the spectral decomposition is not the unique convex combination of pure states that results in a given mixed state which is not pure.[1] The pure states form the extreme set of $\mathcal{S}(\mathcal{H})$. Simple observation gives us also that $\dim_{\mathbb{R}} \mathcal{P}(\mathcal{H}) = 2d - 2$ and $\dim_{\mathbb{R}} \mathcal{S}(\mathcal{H}) = d^2 - 1$.

The complex projective space $\mathbb{CP}^{d-1}$ is endowed with the *Fubini-Study* Kähler metric given by $D_{FS}([\varphi], [\psi]) := \arccos \frac{|\langle\varphi|\psi\rangle|}{\|\varphi\|\|\psi\|}$ for $\varphi, \psi \in \mathcal{H}$ [**24, 66**]. In this metric there is only one geodesic between two pure states unless they are maximally remote (i.e. orthogonal) [**98**, Thm 1]. The transferred metric on $\mathcal{P}(\mathcal{H})$, also called the *Fubini-Study metric*, is given by $D_{FS}(\rho, \sigma) := \arccos \sqrt{\mathrm{tr}(\rho\sigma)}$ for $\rho, \sigma \in \mathcal{P}(\mathcal{H})$. By m_{FS} we denote the unique unitarily invariant measure on $\mathbb{CP}^{d-1}$ or, equivalently, on $\mathcal{P}(\mathbb{C}^d)$.

The outcome of a quantum measurement is nondeterministic: an observable itself defines a set of possible outcomes, but the probabilities of getting these outcomes depend both on the observable and the initial state of the system.

[1] The remarks about convex combinations hold true in infinite dimensional space if we assume that these combinations can be infinite. The convergence of such infinite combination is then defined in the weak sense.

Mathematical description of quantum observable is given by a positive operator-valued measure (POVM) [**34**]:

DEFINITION 1.3. Let $(\Omega, \mathcal{A})$ be a measurable space and let $\mathcal{L}_s^+(\mathcal{H})$ denote the set of self-adjoint positive-semidefinite operators on $\mathcal{H}$. Then the *positive operator-valued measure (POVM)* is defined to be a function $\Pi : \mathcal{A} \to \mathcal{L}_s^+(\mathcal{H})$ such that $\Pi(\Omega) = \mathbb{I}$ and for any (at most) countable family $A_1, A_2, \ldots \subset \mathcal{A}$ of pairwise disjoint sets the equality

$$\sum_{j=1}^{\infty} \Pi(A_j) = \Pi(\bigcup_{j=1}^{\infty} A_j)$$

holds in the sense of weak operator convergence.

The set of possible outcomes is defined by Ω. If the state before the measurement of the observable was ρ, the probability that we get an outcome lying in $A \in \mathcal{A}$ is given by the *Born rule*: $p_A(\rho) := \mathrm{Tr}(\rho\Pi(A))$.

In practice, a POVM is implemented as a projective measurement (PVM, projective-valued measure) on a larger Hilbert space ($\mathcal{H}$ coupled with the so-called *ancilla*). The existence of such measurement is granted by Naimark's dilation theorem [**116**].

From now on we will consider only finite POVMs, i.e. these with finite set of possible outcomes ($|\Omega| < \infty$). In such case by POVM Π we mean a set of operators $\{\Pi_j\}_{j\in\Omega} \subset \mathcal{L}_s^+(\mathcal{H})$ satisfying the identity decomposition:

$$\sum_{j\in\Omega} \Pi_j = \mathbb{I}.$$

A special class of such POVMs are *normalized rank-1* POVMs, where Π_j ($j = 1, \ldots, k$) are rank-1 operators and $\mathrm{Tr}\,(\Pi_j) = \mathrm{const}(j) = d/k$. Necessarily, $k \geq d$ in this case, and there exists an ensemble of pure states $\rho_j = |\phi_j\rangle\langle\phi_j| \in \mathcal{P}\,(\mathcal{H})$ ($j = 1, \ldots, k$) such that $\Pi_j = (d/k)\,\rho_j$. Thus, $\sum_{j=1}^k \rho_j = (k/d)\,\mathbb{I}$, and so a normalized rank-1 POVM can be also defined by a (multi-)set of state vectors $\{|\phi_j\rangle\}_{j=1}^k$ in $\mathcal{H}$ that constitutes a *uniform* (or *normalized*) *tight frame* in $\mathcal{H}$ [**63, 22, 39**], that is an ensemble that fulfills $\sum_{j=1}^k |\langle\psi|\phi_j\rangle|^2 = (k/d)\|\psi\|^2$ for every $|\psi\rangle \in \mathcal{H}$, or, equivalently $\sum_{j=1}^k \mathrm{Tr}\,(\rho_j\sigma) = k/d$ for every $\sigma \in \mathcal{P}\,(\mathcal{H})$. In this case we shall say that ρ_j ($j = 1, \ldots, k$) constitute a POVM. Equivalently, we can define normalized rank-1 POVMs as complex projective 1-designs, where by a *complex projective t-design* ($t \in \mathbb{N}$) we mean an ensemble $\{\rho_j : j = 1, \ldots, k\}$ such that

$$\frac{1}{k^2}\sum_{j,m=1}^{k} f\left(\mathrm{Tr}\left(\rho_j\rho_m\right)\right) = \int_{\mathcal{P}\left(\mathbb{C}^d\right)}\int_{\mathcal{P}\left(\mathbb{C}^d\right)} f\left(\mathrm{Tr}\left(\rho\sigma\right)\right) dm_{FS}\left(\rho\right) dm_{FS}\left(\sigma\right) \qquad (1)$$

for every $f : \mathbb{R} \to \mathbb{R}$ polynomial of degree t or less [**139**].

The special feature of quantum theory is that the quantum measurement generically changes the state. In general, the POVM alone is not sufficient to determine the post-measurement state. This can be determined by defining a *measurement instrument* in the sense of Davies and Lewis [**54**] compatible with Π, however, we are not going here into details, see [**85**, Ch. 5]. Let us just note that in the most standard setup, if the state before the measurement was ρ and the outcome of the measurement was $j \in \Omega$, then the state after measurement is given by

$$\rho' = \frac{\sum_{m=1}^{n_j} M_m^j \rho \left(M_m^j\right)^*}{p_j\left(\rho\right)},$$

where $p_j\left(\rho\right) = \mathrm{Tr}\left(\rho \Pi_j\right)$ and $\left(M_m^j\right)_{m=1}^{n_j} \subset \mathcal{L}(\mathcal{H})$ satisfy $\sum_{m=1}^{n_j} \left(M_m^j\right)^* M_m^j = \Pi_j$. If $n_j = 1$ for every $j \in \Omega$, the measurement is called efficient [**69**]; if, additionally, $M_1^j = \sqrt{\Pi_j}$ we get so called *generalised Lüders instrument* disturbing the initial state in the minimal way [**55**, p.404].

1.3. Bloch representation

Sometimes it may be more convenient to consider the so-called *Bloch (coherence) representation* of quantum states [**24, 23, 131, 14**]. The space of linear operators on $\mathcal{H}$ is endowed with the Hilbert-Schmidt inner product given by $\langle\langle A, B\rangle\rangle_{HS} := \mathrm{Tr}(A^* B)$. The map defined by

$$b : \mathcal{S}(\mathcal{H}) \ni \rho \mapsto \rho - \frac{1}{d}\mathbb{I} \in \mathcal{L}_s^0(\mathcal{H}) \tag{2}$$

provides an affine embedding of mixed states into the (d^2-1)-dimensional real space $\mathcal{L}_s^0(\mathcal{H})$ of self-adjoint traceless operators on $\mathcal{H}$.[2] To be more precise, $b(\mathcal{S}(\mathcal{H}))$ (resp. $b(\mathcal{P}(\mathcal{H}))$) is contained in the ball (resp. sphere) of radius $\sqrt{1-d^{-1}}$:[3]

$$\begin{aligned} \|\rho - \mathbb{I}/d\|_{HS}^2 &= \mathrm{Tr}(\rho - \mathbb{I}/d)^2 = \mathrm{Tr}(\rho^2) - \frac{2}{d}\mathrm{Tr}(\rho) + \frac{1}{d^2}\mathrm{Tr}(\mathbb{I}) \\ &= \mathrm{Tr}(\rho^2) - \frac{2}{d} + \frac{1}{d} \leq 1 - \frac{1}{d} \end{aligned} \tag{3}$$

and the equality holds for pure states only. We will refer to $b(\mathcal{S}(\mathcal{H}))$ as the *Bloch set*. The notions of the *generalized Bloch ball* and the *generalized Bloch sphere* (for $b(\mathcal{P}(\mathcal{H}))$) are also in use. It is clear that $b(\mathcal{P}(\mathcal{H}))$ is a $(2d-2)$-dimensional submanifold of (d^2-1)-dimensional space $\mathcal{L}_s^0(\mathcal{H})$ since it is an affine image of $(2d-2)$-dimensional submanifold of an affine hyperplane of d^2-dimensional real space of self-adjoint operators $\mathcal{L}_s(\mathcal{H})$ consisting of operators of trace 1 (see, e.g. [**73**, Thm 3]).

[2] The map $A \mapsto iA$ allows us to identify $\mathcal{L}_s^0(\mathcal{H})$ with $\mathfrak{su}(d)$, the Lie algebra of $\mathrm{SU}(d)$, consisting of traceless skew-adjoint operators.

[3] The choice of the radius is a question of convention. Another widely used choices are: 1 [**4**], $\sqrt{2(1-d^{-1})}$ [**99**] or $\sqrt{(d-1)/(d+1)}$ [**131**].

The inner products of quantum states and their Bloch images are related in the following way:

$$\begin{aligned}\langle\langle \rho, \sigma \rangle\rangle_{HS} &= \mathrm{Tr}(\rho\sigma) = \mathrm{Tr}((b(\rho) + \mathbb{I}/d)(b(\sigma) + \mathbb{I}/d)) \\ &= \langle\langle b(\rho), b(\sigma) \rangle\rangle_{HS} + 1/d,\end{aligned} \tag{4}$$

for $\rho, \sigma \in \mathcal{S}(\mathcal{H})$. In particular, for the unit vectors $\psi, \phi \in \mathbb{C}^d$ we get:

$$|\langle \psi | \phi \rangle|^2 = \langle\langle b(|\psi\rangle\langle\psi|), b(|\phi\rangle\langle\phi|) \rangle\rangle_{HS} + 1/d. \tag{5}$$

If $d > 2$ then $b(\mathcal{S}(\mathcal{H}))$ is a proper subset of the ball indicated above. This is because there exist operators in the ball $B(0, \sqrt{1 - d^{-1}}) \subset \mathcal{L}_s^0(\mathcal{H})$ such that their images via the inverse map are not positive. To see this let us consider the possible angle α between the Bloch images of two pure states. From (5) we get that α varies from 1, when states coincide, to $\arccos(-1/(d-1))$, when they are orthogonal. Thus the maximal angle decreases with dimension d from π for $d = 2$ through $2\pi/3$ for $d = 3$, and tends to $\pi/2$ as $d \to \infty$.

The space $\mathcal{L}_s^0(\mathcal{H})$ with the Hilbert-Schmidt inner product is an euclidean real space, thus most often the Bloch representation is considered as a map into $\mathbb{R}^{d^2-1}$. Since $\dim_{\mathbb{C}} \mathcal{L}(\mathcal{H}) = d^2 = \dim_{\mathbb{R}} \mathcal{L}_s(\mathcal{H})$, it is possible to choose an orthogonal basis $\{E_i\}_{i=0}^{d^2-1}$ for $\mathcal{L}(\mathcal{H})$ consisting of self-adjoint operators. If we put $E_0 = \mathbb{I}$, then, by the orthogonality, the remaining basis elements are traceless. Additionally, we assume that $\|E_i\|_{HS}^2 = d$ for $i = 1, \ldots, d^2 - 1$. Then any $\rho \in \mathcal{S}(\mathcal{H})$ can be written as

$$\rho = \frac{1}{d} \sum_{i=1}^{d^2} \mathrm{Tr}(\rho E_i) E_i = \frac{1}{d} \left(\mathbb{I} + \vec{b}_\rho \cdot \vec{E} \right), \tag{6}$$

where $\vec{b}_\rho = (\mathrm{Tr}(\rho E_1), \ldots, \mathrm{Tr}(\rho E_{d^2-1}))$ and $\vec{E} = \{E_1, \ldots, E_{d^2-1}\}$. Obviously $b(\rho) = d^{-1} \vec{b}_\rho \cdot \vec{E}$ and $\langle\langle b(\rho), b(\sigma) \rangle\rangle_{HS} = d^{-1} \vec{b}_\rho \cdot \vec{b}_\sigma$ for $\rho, \sigma \in \mathcal{S}(\mathcal{H})$, where by dot we denote the standard euclidean inner product in $\mathbb{R}^{d^2-1}$. We will refer to $\vec{b}_\rho$ as the *Bloch vector* corresponding to the state ρ. Throughout the thesis we shall often use normalized Bloch vectors for greater convenience and denote the set of normalized Bloch vectors in $S^{d^2-2} \subset \mathbb{R}^{d^2-1}$ by $B(d)$.

The Bloch representation in $\mathbb{R}^{d^2-1}$ depends on the choice of basis in $\mathcal{L}_s^0(\mathcal{H})$. For the greater convenience such bases are often written in a matrix form. The most commonly used are the *Pauli matrices* for $d = 2$, the *Gell-Mann matrices* for $d = 3$ and the *generalized Gell-Mann matrices* for $d > 3$ [**26**].

EXAMPLE 1.1 (Pauli matrices and Bloch sphere[4]). We consider $\mathcal{H} = \mathbb{C}^2$ with the standard orthonormal basis $\{|0\rangle, |1\rangle\}$. The Pauli matrices σ_x, σ_y and σ_z (sometimes denoted also by X, Y and Z), introduced in 1927 to give a mathematical

[4] Called also *Riemann-Majorana-Bloch sphere* or *Bloch-Poincaré sphere.*

description of spin [**118**], are given by:

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{7}$$

They are obviously traceless and self-adjoint and it is easy to check that $\langle\langle \sigma_i, \sigma_j \rangle\rangle_{HS} = 2\delta_{ij}$ for $i, j \in \{x, y, z\}$.

The Bloch set in dimension two forms the whole unit ball in $\mathbb{R}^3$, not only a proper subset of it. To see this we need to answer the question, when the operator of the form $\rho = (\mathbb{I} + \vec{b} \cdot \vec{\sigma})/2$ is positive? It is enough to observe that the eigenvalues of ρ are $\lambda_\pm = (1 \pm \|\vec{b}\|)/2$, and they are both positive if and only if $\|\vec{b}\| \leq 1$. The Bloch vectors corresponding to the pure states form then the unit sphere in $\mathbb{R}^3$. Since $|\langle\psi|\phi\rangle|^2 = (\vec{b}_\psi \cdot \vec{b}_\phi)/2$, the antipodal points on the Bloch sphere correspond to the orthogonal states. ■

Let us recall that a normalized rank-1 POVM consists of subnormalized projectors $\Pi_j = (d/k)\rho_j$ $(j = 1, \ldots, k)$. The equality $\sum_{j=1}^k \rho_j = (k/d)\, \mathbb{I}$ is in turn equivalent to $\sum_{j=1}^k b(\rho_j) = 0$, which gives the following well known simple characterization of normalized rank-1 POVMs in the language of Bloch vectors:

FACT 1.2. The generalized Bloch representation gives a one-to-one correspondence between finite normalized rank-1 POVMs and finite (multi-)sets of points in $b\left(\mathcal{P}(\mathbb{C}^d)\right)$ with its center of mass at 0.

It follows from (4) that the probabilities of the measurement outcomes in the generalized Bloch representation take the form

$$p_j(\rho) = (d/k)\,\mathrm{Tr}\,(\rho_j \rho) = (d \cdot \langle\langle b(\rho_j), b(\rho) \rangle\rangle_{HS} + 1)/k = (\vec{b}_{\rho_j} \cdot \vec{b}_\rho + 1)/k \tag{8}$$

for $\rho \in \mathcal{P}\left(\mathbb{C}^d\right)$ and $j = 1, \ldots, k$. Obviously, the probability of obtaining j-th outcome vary from 0, when the initial state is orthogonal to ρ_j, to d/k, when it coincides with ρ_j. In consequence, any outcome cannot be certain for given input state unless the measurement is projective (in which case $k = d$).

CHAPTER 2

Symmetry

> Nothing is so stifling as symmetry. Symmetry is boredom, the quintessence of mourning. Despair yawns. There is something more terrible than a hell of suffering – a hell of boredom.
>
> (Victor Hugo, *Les Misérables*)

This chapter is devoted to the concept of symmetry understood as the group-invariance. We introduce the notion of highly symmetric sets and apply it to quantum measurements. In particular, we provide a full characterization of such measurements in dimension two. The chapter contains also a description of informationally complete measurement and give an insight into the algebraic structure of symmetric informationally complete measurements (SIC-POVMs) that are covariant with respect to the Weyl-Heisenberg group.

2.1. Symmetry in metric spaces

Let (X, r) be a metric space. By $\mathrm{Isom}(X)$ we denote the set of all isometries of X. We say that $f \in \mathrm{Isom}(X)$ is a *symmetry* of $S \subset X$ if it leaves S invariant and we denote the group of symmetries of S by $\mathrm{Sym}(S)$.

Definition 2.1. We say that S is *symmetric* if $\mathrm{Sym}(S)$ acts transitively on S, i.e. for every $x, y \in S$ there exists $f \in \mathrm{Sym}(S)$ such that $f(x) = y$.

Definition 2.2. [**60**] We say that S is a *resolving set* if $r(a, x) = r(b, x)$ for every $x \in S$ implies $a = b$, for $a, b \in X$.

Proposition 2.1. *If S is symmetric and resolving, then $f|_S = g|_S$ implies $f = g$ for every $f, g \in \mathrm{Sym}(S)$. Moreover, if S is finite, then $\mathrm{Sym}(S)$ is finite.*

Proof. Let $f, g \in \mathrm{Sym}(S)$, $f|_S = g|_S$, and $a \in X$. Then, for every $x \in S$ we have $r(fa, x) = r(a, f^{-1}x) = r(a, g^{-1}x) = r(ga, x)$. Hence $fa = ga$. Now, if $|S| = k$, then $\mathrm{Sym}(S)$ is a subgroup of the symmetric group S_k, and so is finite. $\square$

In order to introduce the notion of *highly symmetric* sets we need to recall some basic definitions from the group action theory, see, e.g. [**64**]. Let G be a group acting on X and let $x \in X$. By the *orbit* of x we mean the set $Gx := \{gx : g \in G\}$ and by the *stabilizer* of x the set $G_x := \{h \in G : hx = x\}$. Let us observe that

$G_{gx} = gG_xg^{-1}$ and so all the points from a single orbit have the same stabilizers up to the conjugacy. We say that the points from X are of the same *isotropy type* if their stabilizers are conjugated. The points of the same isotropy type as x form the *orbit stratum* Σ_x. The decomposition of X into orbit strata is called the *orbit stratification*. Clearly, it induces a stratification of the orbit space X/G. The natural partial order on the set of all conjugacy classes of subgroups of G induces the order on the set of strata, namely, $\Sigma_x \preceq \Sigma_y$ if and only if there exists $g \in G$ such that $G_x \subset gG_yg^{-1}$ for $x, y \in X$, so that the maximal strata consist of points with maximal stabilizers.

Assume now that S is symmetric and consider the action of the group $\mathrm{Sym}\,(S)$ on X. Clearly, the whole set S is contained in one orbit and hence in one stratum.

DEFINITION 2.3. We say that S is *highly symmetric* in (X, r) if and only if the stratum it is contained in is maximal.

EXAMPLE 2.1. The sets S_t of vertices of the equilateral triangle and S_h – of the hexagon presented in Fig. 1 have the same symmetry group D_{3h}. Since it acts transitively on these sets, they are both symmetric. However, S_t is contained in the maximal stratum, and so it is also highly symmetric in $\mathbb{R}^2$, while S_h is not.■

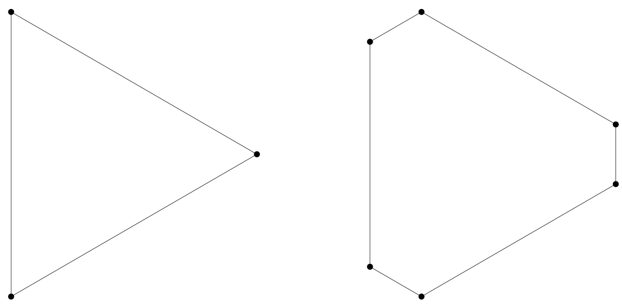

FIGURE 1. An example of highly symmetric set (left) and symmetric but not highly symmetric set (right).

A symmetric set is highly symmetric if and only if it has not a non-trivial factor of an equal or higher symmetry:

PROPOSITION 2.2. *Let $S \subset X$ be symmetric. Then S is highly symmetric if and only if every $\mathrm{Sym}\,(S)$-equivariant map $h : S \to X$ (i.e. such that $gh(x) = h(gx)$ for every $g \in \mathrm{Sym}\,(S)$ and for some (and hence all) $x \in S$) is one-to-one.*

PROOF. If $|S| = 1$, then the proposition is trivial. Assume that $|S| \geq 2$ and put $G := \mathrm{Sym}\,(S)$. If S is not highly symmetric, then there exist $x \in S = Gx$ and $y \notin S$ such that $G_x \subsetneq G_y$. Put $h(gx) = g(y)$ for $g \in G$. Clearly h is not one-to-one, since otherwise $G_y \subset G_x$, which is a contradiction. On the other hand, take $h : S \to X$ such that $gh(x) = h(gx)$ for all $x \in S$ and $g \in \mathrm{Sym}\,(S)$. If there exist $x \in S$ and $g \in \mathrm{Sym}(S)$ such that $x \neq gx$ and $h(x) = h(gx)$, then we have $G_x \subset G_{h(x)}$ and $g \in G_{h(x)} \backslash G_x$, a contradiction. □

It is interesting that an analogous idea was explored almost fifty years ago by Zajtz who defined so called *primitive geometric objects* in quite similar manner as highly symmetric sets defined above and proved the fact parallel to Proposition 2.2 [**167**, Thm 1].

2.2. Symmetric quantum measurements

To apply these general definitions to normalized rank-1 POVMs, note that from the celebrated Wigner theorem [**163**] it follows that for every separable Hilbert space $\mathcal{H}$ the group of isometries of $(\mathcal{P}(\mathcal{H}), D_{FS})$ (*quantum symmetries*) is isomorphic to the projective unitary-antiunitary group $\mathrm{PUA}(\mathcal{H})$, consisting of unitary and antiunitary transformations of $\mathcal{H}$ defined up to phase factors, see also [**40, 41, 97, 66, 74**]. To be more precise, each such isometry is given by the map $\sigma_U : \mathcal{P}(\mathcal{H}) \ni \rho \to U\rho U^* \in \mathcal{P}(\mathcal{H})$ for a unitary or antiunitary U, and two such isometries coincide if and only if the corresponding transformations differ only by a phase. Equivalence classes of unitary isometries form a normal subgroup of $\mathrm{PUA}(\mathcal{H})$ of index 2, namely the projective unitary group $\mathrm{PU}(\mathcal{H})$. Clearly, every such isometry can be uniquely extended to a continuous affine map on $\mathcal{S}(\mathcal{H})$.

If $\mathcal{H} = \mathbb{C}^d$, then the generalized Bloch representation gives a one-to-one correspondence between the compact group $\mathrm{PUA}(d)$ and the group of isometries of the unit sphere in (d^2-1)-dimensional real vector space $\mathcal{L}_s^0(\mathbb{C}^d)$ endowed with the Hilbert-Schmidt product, whose action leaves the Bloch set $b(\mathcal{S}(\mathbb{C}^d))$ invariant. This correspondence is given by $[U] \to \left\{\rho \to U\rho U^* : \rho \in \mathcal{L}_s^0(\mathbb{C}^d)\right\}$ for $U \in \mathrm{UA}(d)$ (the unitary case is shown in [**14**] and it can be easily generalized to the antiunitary case). Hence $\mathrm{PUA}(d)$ is isomorphic to a subgroup of the orthogonal group $O(d^2-1)$. Moreover, m_{FS} is the unique $\mathrm{PUA}(d)$-invariant measure on $\mathcal{P}\left(\mathbb{C}^d\right) \simeq \mathbb{CP}^{d-1}$. In particular, for $d = 2$, we have $\mathrm{PUA}(2) \simeq O(3)$, and so all quantum symmetries of qubit states can be interpreted as rotations (for unitary symmetries, as $\mathrm{PU}(2) \simeq SO(3)$), reflections or rotoreflections of the three dimensional Euclidean space.

Taking this into account we can transfer the notions of symmetry and high symmetry from $\mathcal{P}\left(\mathbb{C}^d\right)$ to finite normalized rank-1 POVMs in $\mathbb{C}^d$. Let $\Pi = (\Pi_j)_{j=1,\dots,k}$ be a finite normalized rank-1 POVM in $\mathbb{C}^d$ and S be a corresponding set of pure quantum states. We say that

Definition 2.4. Π is a *symmetric POVM* $\Leftrightarrow$ S is symmetric in $(\mathcal{P}(\mathbb{C}^d), D_{FS})$.

Definition 2.5. Π is a *highly symmetric POVM* (*HS-POVM*) $\Leftrightarrow$ S is highly symmetric in $(\mathcal{P}(\mathbb{C}^d), D_{FS})$.

For finite normalized rank-1 measurements symmetric POVMs coincide, as we shall show below, with *group covariant POVMs* introduced by Holevo [**88**] and studied since then by many authors.

DEFINITION 2.6. We say that a measurement $\Pi = (\Pi_j)_{j=1,\ldots,k}$ is *G-covariant* for a group G if and only if there exists $G \ni g \to \sigma_{U_g} \in \mathrm{PUA}\,(d)$, a *projective unitary-antiunitary representation* of G (i.e. a homomorphism from G to $\mathrm{PUA}\,(d)$), and a surjection $s : G \to \{1, \ldots, k\}$ such that $\sigma_{U_g}(\Pi_{s(h)}) = U_g \Pi_{s(h)} U_g^* = \Pi_{s(gh)}$ for all $g, h \in G$.

For the greater convenience, we can assume that Π is a multiset, and so we can label its elements by g instead of $s(g)$: $\Pi = (\Pi_g)_{g\in G}$. In order to guarantee that $\sum_{g\in G} \Pi_g = \mathbb{I}$ we need to put $\Pi_g = (|s(G)|/|G|)\Pi_{s(g)}$.

DEFINITION 2.7. We say that $|\phi\rangle \in \mathbb{C}^d$ is a *fiducial vector* for a G-covariant finite normalized rank-1 POVM Π if $\|\phi\| = 1$ and $\Pi_g = (d/|G|)\sigma_{U_g}(|\phi\rangle\langle\phi|)$.

Let Π be a finite normalized rank-1 POVM in $\mathbb{C}^d$ and S be a corresponding set of pure quantum states. It is clear that a symmetric finite normalized rank-1 POVM is $\mathrm{Sym}\,(S)$-covariant, and, conversely, if a finite normalized rank-1 POVM is G-covariant, then $\left(\sigma_{U_g}\right)_{g\in G}$ is a subgroup of the group of isometries of $\left(\mathcal{P}\left(\mathbb{C}^d\right), D_{FS}\right)$, acting transitively on the corresponding (multi-)set of pure states. We call the representation *irreducible* if and only if $\mathbb{I}/d$ is the only element of $\mathcal{S}\left(\mathbb{C}^d\right)$ invariant under action of the representation. It follows from the version of Schur's lemma for unitary-antiunitary maps [**61**, Thm II] that this definition coincides with the classical one. Irreducibility of the representation can be also equivalently expressed as follows: for any pure state $\rho \in \mathcal{P}\left(\mathbb{C}^d\right)$ its orbit under the action of the representation generates a rank-1 G-covariant POVM, i.e. $\frac{1}{|G|}\sum_{g\in G} \sigma_{U_g}(\rho) = \mathbb{I}/d$, see also [**156**].

Our definition of highly symmetric POVMs resembles the definition of highly symmetric frames introduced by Broome and Waldron [**30, 31, 158**]. However, they consider subsets of $\mathbb{C}^d$ rather than $\mathbb{CP}^{d-1}$ and unitary symmetries rather than projective unitary-antiunitary symmetries.

Another important class of POVMs is characterized by the possibility of reconstruction of the initial state based on the measurement statistics.

DEFINITION 2.8. We call a POVM $\Pi = (\Pi_j)_{j=1,\ldots,k}$ *informationally complete* (resp. *purely informationally complete*) if the conditions $\mathrm{Tr}(\rho\Pi_j) = \mathrm{Tr}(\sigma\Pi_j)$ $(j = 1, \ldots, k)$ imply $\rho = \sigma$ for every input states $\rho, \sigma \in \mathcal{S}(\mathbb{C}^d)$ (resp. $\mathcal{P}(\mathbb{C}^d)$). We use abbreviated form *IC-POVM* for informationally complete POVM.

Since we need $d^2 - 1$ independent parameters to describe uniquely a quantum state, any IC-POVM must contain at least d^2 elements. IC-POVMs consisting of exactly d^2 elements are called *minimal*. Among them the SIC-POVMs deserve special attention:

Definition 2.9. We say that POVM $\{\Pi_j\}_{j=1}^{d^2}$ is a *symmetric informationally complete POVM* (*SIC-POVM*) if it consists of d^2 subnormalized rank-1 projectors $\Pi_j = |\phi_j\rangle\langle\phi_j|/d$ with equal pairwise Hilbert-Schmidt inner products:

$$\mathrm{Tr}(\Pi_i\Pi_j) = \frac{|\langle\phi_i|\phi_j\rangle|^2}{d^2} = \frac{1}{d^2(d+1)} \quad \text{for } i \neq j. \tag{9}$$

Let us note that the above definition may be misleading since 'symmetric informationally complete' does not mean 'symmetric (in the sense of Definition 2.4) and informationally complete'. An example of POVM which is both symmetric and informationally complete, but is not a SIC-POVM is given in Example 2.2. On the other hand, all known SIC-POVMs are group-covariant (most of them with respect to the Weyl Heisenberg group, see Sect. 2.4) and thus symmetric.

The IC-POVMs were introduced by Prugovečki [**122**] and were later studied e.g. by Busch [**33**], Schroeck [**138**], D'Ariano et al. [**10**] and Scott [**139**]. The objects called now SIC-POVMs have been examined firstly in the context of the sets consisting of maximal number of d^2 *equiangular lines* in $\mathbb{C}^d$ or the complex *spherical 2-designs* with d^2 elements. The equiangular lines in the Euclidean space have been studied by mathematicians since 1948, firstly using the terminology of elliptic geometry [**80**]. Most of the later papers covered just real case, e.g. [**104**] until more general considerations by Hoggar [**86**] made in the context of t-designs. The notion of SIC-POVMs has been introduced by Renes et al. in 2003 [**126**], but they have been studied previously (in 1999) by Zauner in his PhD Thesis [**168**] under the name of *regular quantum designs with degree* 1.[1] Since then the question whether there exist maximal sets of equiangular lines in every complex dimension d (i.e. whether there exist SIC-POVMs in every dimension) has been getting the increased attention of quantum physicists (see, e.g. [**9**]). The problem remains open, but there is strong belief that the answer is confirmatory, supported by the numerical results up to $d = 67$ [**140**]. The analytical solutions are known for dimensions $d = 2, 3$ [**57**], $4, 5$ [**168**], 6 [**75**], 7 [**3**], 8 [**86**], $9 - 15$ [**76, 77, 78**], 16 [**5**], 19 [**3**], 24 [**140**], 28 [**6**], 35 and 48 [**140**]. To realize why this problem is so difficult let us observe that the Bloch representation of a SIC-POVM corresponds to the set of vertices of the regular (d^2-1)-simplex in $\mathbb{R}^{d^2-1}$ that need to be inscribed into the $(2d-2)$-dimensional subset of the (d^2-2)-sphere. On the other hand, the existence of minimal IC-POVMs (but not SIC-POVMs) is confirmed in any dimension, one of the simpler constructions can be found in [**68**].

The next proposition clarifies the relations between the properties of the set of pure states constituting a finite normalized rank-1 POVM and the properties

[1]Despite the fact that some ideas in [**126**] and [**168**] were very similar, Renes et al. have worked completely independently. The German language, in which Zauner's dissertation had been written, was the probable cause why four years later Renes et al. were still unaware of his results, even though his dissertation was available online.

of its Bloch representation. It provides necessary and sufficient conditions for informational completeness and purely informational completeness:

PROPOSITION 2.3. *Let* $\Pi = (\Pi_j)_{j=1,\ldots,k}$ *be a finite normalized rank*-1 *POVM in* $\mathbb{C}^d$ *and* $S := \{\rho_j : j = 1, \ldots, k\}$ *be a corresponding set of pure quantum states, i.e.* $\rho_j \in \mathcal{P}(\mathbb{C}^d)$ *and* $\Pi_j = (d/k)\,\rho_j$ *for* $j = 1, \ldots, k$. *Let us consider the following properties:*

a) S *is a complex projective* 2*-design;*
b) $b\,(S)$ *is a normalized tight frame in* $\mathcal{L}_s^0(\mathbb{C}^d)$*;*
c) $b\,(S)$ *is a spherical* 2*-design in* $\mathcal{L}_s^0(\mathbb{C}^d)$*;*
d) Π *is informationally complete;*
e) $b\,(S)$ *generates* $\mathcal{L}_s^0(\mathbb{C}^d)$*;*
f) $b\,(S)$ *is a frame in* $\mathcal{L}_s^0(\mathbb{C}^d)$*;*
g) Π *is purely informationally complete;*
h) S *is a resolving set in* $(\mathcal{P}(\mathbb{C}^d), D_{FS})$*;*
i) $b\,(S)$ *is a resolving set in* $(B\,(d)\,, D_B)$.

Then a) $\Leftrightarrow$ *b*) $\Leftrightarrow$ *c*) $\Rightarrow$ *d*) $\Leftrightarrow$ *e*) $\Leftrightarrow$ *f*) $\Rightarrow$ *g*) $\Leftrightarrow$ *h*) $\Leftrightarrow$ *i*). *Moreover, if* $d = 2$, *then g*) $\Rightarrow$ *d*).

PROOF. It is obvious that *b*) $\Rightarrow$ *f*) and *d*) $\Rightarrow$ *g*). The proof of *a*) $\Leftrightarrow$ *b*) can be found in [**139**, Prop. 13], *b*) $\Leftrightarrow$ *c*) in [**159**, p. 5] and *d*) $\Leftrightarrow$ *e*) in [**85**, Prop. 3.51]. It is well known that in finite dimensional spaces frames are generating sets, hence *e*) $\Leftrightarrow$ *f*). Furthermore, *g*) $\Leftrightarrow$ *h*) $\Leftrightarrow$ *i*) follows from the fact that the distances D_{FS} and D_B are ordinally equivalent, and from the equality $\mathrm{Tr}\,(\rho\sigma) = \cos^2 D_{FS}\,(\rho, \sigma)$ for $\rho, \sigma \in \mathcal{P}(\mathbb{C}^d)$. Moreover, for $d = 2$ the notions of purely informational completeness and informational completeness coincide [**84**, Remark 1]. □

REMARK 2.1. A POVM that satisfies *a*) (or, equivalently, *b*) or *c*)) is called *tight informationally complete POVM* [**139**]. In particular, SIC-POVMs are tight.

Note that *d*) does not imply *b*), even if S is symmetric and $d = 2$:

EXAMPLE 2.2. Let us consider $S \subset \mathcal{P}\,(\mathbb{C}^2)$ such that $b(S) = \{2^{-1/2}(e_1 \pm e_2), 2^{-1/2}(-e_1 \pm e_3)\}$, where $\{e_1, e_2, e_3\}$ is any orthonormal basis of $\mathcal{L}_s^0(\mathbb{C}^2)$. Then $b\,(S)$ is a tetragonal disphenoid (see Fig. 2) with the antiprismatic symmetry group D_{2d}. Clearly, $b\,(S)$ is a frame in $\mathcal{L}_s^0(\mathbb{C}^2)$, but simple calculations show that it is not tight. ■

On the other hand, one can prove *d*) $\Rightarrow$ *b*), under the additional assumption that the natural action of $\mathrm{Sym}\,(S)$ on $\mathcal{L}_s^0(\mathbb{C}^d)$ is irreducible, applying [**156**, Thm 6.3]. Moreover, as we shall see in the next section, all the conditions above are equivalent if S is highly symmetric and $d = 2$.

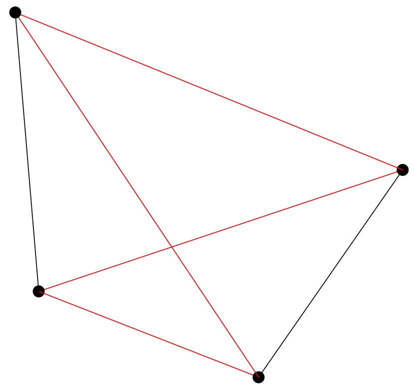

FIGURE 2. A tetragonal disphenoid. Edges of the same length are of the same colour.

2.3. Classification of highly symmetric POVMs in dimension 2

THEOREM 2.4. *There are only eight types of HS-POVMs in two dimensions, seven exceptional informationally complete HS-POVM represented in* $\mathbb{R}^3$ *by five Platonic solids (convex regular polyhedra): the* ***tetrahedron****,* ***cube****,* ***octahedron****,* ***icosahedron*** *and* ***dodecahedron*** *and two convex quasi-regular polyhedra: the* ***cuboctahedron*** *and* ***icosidodecahedron****, and an infinite series of non informationally complete HS-POVMs represented in* $\mathbb{R}^3$ *by* ***regular polygons****, including* ***digon****.*

PROOF. Let $S = \{\rho_j : j = 1, \ldots, k\} \subset \mathcal{P}(\mathbb{C}^2) \simeq \mathbb{CP}$ constitute a HS-POVM, and let $B := b(S) \subset S^2$. Put $G := \mathrm{Sym}\,(B)$. Then it follows from the equivalence $d) \Leftrightarrow e)$ in Proposition 2.3 that either B is contained in a proper (one- or two-dimensional) subspace of $\mathbb{R}^3$, or the POVM is informationally complete and, according to the implication $d) \Rightarrow h)$ in Proposition 2.3 and Proposition 2.1, G is finite.

If G is infinite, then necessarily the stabilizer of any element $x \in B$ has to be infinite, since otherwise the whole orbit of x would be infinite. As the only linear isometries of $\mathbb{R}^3$ leaving possibly x invariant are either rotations about the axis l_x through x, or reflections in any plane containing l_x, the stabilizer G_x has to contain an infinite subgroup of rotations about l_x. Thus the orbit of any point beyond l_x under G must be infinite. In consequence, $B = \{-x, x\}$, and $G = D_{\infty h} \simeq O\,(2) \times C_2$.

If G is finite, it must be one of the point groups, i.e. finite subgroups of $O\,(3)$. The complete characterization of such subgroups has been known for very long time [**141**]: there exist seven infinite families of axial (or prismatic) groups C_n, C_{nv}, C_{nh}, S_{2n}, D_n, D_{nd} and D_{nh}, as well as seven additional polyhedral (or spherical) groups: T (chiral tetrahedral), T_d (full tetrahedral), T_h (pyritohedral), O (chiral octahedral), O_h (full octahedral), I (chiral icosahedral) and I_h (full icosahedral). Analysing their standard action on S^2 (see, e.g. [**129, 107, 114, 171, 123**]), one can find in all cases the orbits with maximal stabilizers. Gathering this information together, we get all highly symmetric finite subsets of S^2, and so all HS-POVMs in two dimensions. These sets are listed in Tab. 1 together with their symmetry groups and the stabilizers of their elements with respect to these symmetry groups. For all but the first two types of HS-POVMs, the symmetry group G is a polyhedral group, and so it acts irreducibly on $\mathbb{R}^3$. Hence, B must be a tight frame in all these cases. $\square$

convex hull of the orbit	cardinality of the orbit	group	stabilizer
digon	2	$D_{\infty h}$	$C_{\infty v}$
regular n-gon ($n \geq 3$)	n	D_{nh}	C_{2v}
tetrahedron	4	T_d	C_{3v}
octahedron	6	O_h	C_{4v}
cube	8	O_h	C_{3v}
cuboctahedron	12	O_h	C_{2v}
icosahedron	12	I_h	C_{5v}
dodecahedron	20	I_h	C_{3v}
icosidodecahedron	30	I_h	C_{2v}

Table 1. HS-POVMs in dimension two, with their cardinalities, symmetry groups and stabilizers of elements (in Schoenflies notation).

Remark 2.2. We have just shown that if $S \subset \mathcal{P}(\mathbb{C}^2)$ constitutes an informationally complete HS-POVM in dimension two, then $b(S)$ is a spherical 2-design. However, it follows from [**46**, Thm 2] and the form of corresponding group invariant polynomials (listed in Sect. 4.1.4) that if $\mathrm{Sym}(b(S)) = O_h$, then $b(S)$ is a spherical 3-design and if $\mathrm{Sym}(b(S)) = I_h$, then $b(S)$ is a spherical 5-design.

Classification of all finite symmetric subsets of S^2 and, in consequence, all symmetric normalized rank-1 POVMs in two dimensions, is of course more complicated than for highly symmetric case. In particular, the number of such non-isometric subsets is uncountable. However, since each symmetric subset generates a *vertex-transitive polyhedron* in three-dimensional Euclidean space (and each such polyhedron is a symmetric set generating symmetric normalized rank-1 POVM), the task reduces to classifying such polyhedra, which was done by Robertson and Carter in the 1970s, see [**129, 130, 128, 47**]. They proved that the transitive polyhedra in $\mathbb{R}^3$ can be parameterized (up to isometry) by metric space (with the Hausdorff distance under the action of Euclidean isometries related closely to the Gromov-Hausdorff distance, see [**111**]), which is a two-dimensional CW-complex with 0-cells corresponding exactly to highly symmetric subsets of S^2.

Note that not only 'regular polygonal' POVMs (e.g. the trine or 'Mercedes-Benz' measurement for $n = 3$ [**95**] and the 'Chrysler' measurement for $n = 5$ [**164**]), but also 'Platonic solid' POVMs have been considered earlier by several authors in various contexts, see for instance [**38, 42, 56, 32**].

2.4. Weyl-Heisenberg SIC-POVMs

In this section we consider the group-covariant SIC-POVMs with respect to the *finite Weyl-Heisenberg* (WH) *group*.[2] The assumption of WH-covariance is not very restrictive since all known SIC-POVMs are group-covariant and most of them are WH-covariant, with the only exception for $d = 8$, described in [**168**]. In particular, if d is prime then group-covariance implies WH-covariance [**172**, Lemma 1].

The finite Weyl-Heisenberg group H_d can be defined by the following presentation:

$$\langle x, y, z | x^d = y^d = z^d = 1, zx = xz, zy = yz, x^r y^s = z^{rs} y^s x^r, z = xyx^{-1}y^{-1} \rangle.$$

In order to introduce its projective unitary representation in $\mathbb{C}^d$, let us denote an orthonormal basis in $\mathbb{C}^d$ by $|e_0\rangle, |e_1\rangle, \ldots |e_{d-1}\rangle$. We define the operators T and S as follows:

$$S|e_r\rangle := |e_{r\oplus 1}\rangle, \quad T|e_r\rangle := \omega^r |e_r\rangle,$$

where $r = 0, \ldots, d-1$, $\oplus$ denotes the addition modulo d and $\omega := \exp(2\pi i/d)$. They are both traceless and unitary, and, while written in the matrix form, they are considered as generalized Pauli matrices σ_x and σ_z. Note, however, that in dimensions $d > 2$ they are no longer Hermitian. Commonly used names are *shift operator* (*matrix*) and *phase* or *clock operator* (*matrix*). We define also

$$D_{\mathbf{p}} = D_{(p_1,p_2)} := \tau^{p_1 p_2} S^{p_1} T^{p_2},$$

where $\tau := -\exp(\pi i/d)$ and $\mathbf{p} = (p_1, p_2) \in \mathbb{Z}^2$. We have

$$D_{\mathbf{p}}^* = D_{-\mathbf{p}} \quad \text{and} \quad D_{\mathbf{p}} D_{\mathbf{q}} = \tau^{\langle \mathbf{p}, \mathbf{q} \rangle} D_{\mathbf{p}+\mathbf{q}}$$

for all $\mathbf{p}, \mathbf{q} \in \mathbb{Z}^2$, where $\langle \mathbf{p}, \mathbf{q} \rangle = p_2 q_1 - p_1 q_2$ (symplectic form). Operators $D_{\mathbf{p}}$ are called *discrete Weyl operators* (*Weyl matrices*) or *generalized Pauli matrices.*

The Weyl-Heisenberg group is irreducibly and faithfully represented by the elements of the form $\omega^{p_3} S^{p_1} T^{p_2}$, where $p_1, p_2, p_3 \in \mathbb{Z}_d$ (a homomorphism $h : H_d \to \{\omega^{p_3} S^{p_1} T^{p_2} | p_1, p_2, p_3 \in \mathbb{Z}_d\}$ on the generating elements is given by

[2] Mathematicians use just Heisenberg's name. In the physical literature this group is most commonly called the Weyl-Heisenberg group, partially because the authors most often refer to the concrete representations in $\mathbb{C}^d$, with the use of the Weyl matrices, and not to the abstract group. The name of the *generalized Pauli* (GP) group is also in use.

$h(x) := S, h(y) := T, h(z) := \omega\mathbb{I})$. We obtain the projective representation taking the equivalence classes $[\omega^{p_3} S^{p_1} T^{p_2}] = [D_{(p_1,p_2)}]$. Note that the map $(p_1, p_2) \mapsto [D_{(p_1,p_2)}]$ provides also the projective unitary representation of $\mathbb{Z}_d \times \mathbb{Z}_d$ on $\mathbb{C}^d$ and so the WH-covariant SIC-POVMs are sometimes also considered as covariant with respect to $\mathbb{Z}_d \times \mathbb{Z}_d$.

Let us recall some definitions from the group theory. For groups G and H such that $H \subset G$ the *normalizer* of H in G is defined to be $N_H(G) := \{g \in G : gH = Hg\}$. If group F acts on group G, we can define the (*outer*) *semidirect product* of F and G, namely the group $F \ltimes G$ with the operation $* : (F \ltimes G) \times (F \ltimes G) \to F \ltimes G$ defined by $(\mathcal{F}_1, g_1) * (\mathcal{F}_2, g_2) = (\mathcal{F}_1\mathcal{F}_2, g_1(\mathcal{F}_1 g_2))$.

We shall consider the normalizer of the Weyl-Heisenberg group in the group $\mathrm{UA}(d)$ of all unitary and antiunitary operators on $\mathbb{C}^d$, the so-called *extended Clifford group* $\mathrm{EC}(d)$. This group is a disjoint union of the normalizer of the WH group in $\mathrm{U}(d)$ denoted by $\mathrm{C}(d)$ and called *Clifford* (or *Jacobi*) *group*, and the set $\mathrm{C}^*(d)$ of antiunitary operators in $\mathrm{EC}(d)$. Every element of $\mathrm{C}^*(d)$ can be written in the form JU, where $U \in \mathrm{C}(d)$ and J is the antilinear map defined by $J(\sum_{j=0}^{d-1} \alpha_j |e_j\rangle) = \sum_{j=0}^{d-1} \overline{\alpha_j} |e_j\rangle$ [**3**]. Moreover, we denote by $\mathrm{ESL}(2, \mathbb{Z}_d)$ the *extended special linear group* of all 2×2 matrices over $\mathbb{Z}_d$ with determinant ± 1 (mod d) and by $\mathrm{I}(d)$ the group of unitary multiples of identity operator on $\mathbb{C}^d$.

The connection between the extended Clifford group and the extended special linear group is given by the following theorem by Appleby:

THEOREM 2.5 (Appleby [**3**, Thm 2]). *For odd dimension d there exists a unique isomorphism $f_E : \mathrm{ESL}(2, \mathbb{Z}_d) \ltimes (\mathbb{Z}_d \times \mathbb{Z}_d) \to \mathrm{EC}(d)/\mathrm{I}(d)$ that for any $(\mathcal{F}, \mathbf{r}) \in \mathrm{ESL}(2, \mathbb{Z}_d) \ltimes (\mathbb{Z}_d \times \mathbb{Z}_d)$ and $U \in f_E(\mathcal{F}, \mathbf{r})$ fulfills the condition*

$$U D_{\mathbf{p}} U^* = \omega^{\langle \mathbf{r}, \mathcal{F}\mathbf{p} \rangle} D_{\mathcal{F}\mathbf{p}} \tag{10}$$

for all $\mathbf{p} \in \mathbb{Z}_d \times \mathbb{Z}_d$. Moreover, U is unitary if $\det \mathcal{F} = 1$ and antiunitary if $\det \mathcal{F} = -1$.[3]

Let us consider $U \in f_E(\mathcal{F}, \mathbf{r})$, where $\mathcal{F}$ is such that $\det \mathcal{F} = 1$, $\mathrm{Tr}\mathcal{F} \equiv -1$ (mod d), $\mathcal{F} \neq \mathcal{I}$ and $\mathbf{r} \in \mathbb{Z}_d \times \mathbb{Z}_d$. Then U is unitary and $[U^3] = [\mathbb{I}]$ [**3**, Lemma 7], and so one can choose the phase factor of U in a way that $U^3 = \mathbb{I}$. Such unitary operator will be called *canonical order* 3 *unitary* and denoted by $U_{(\mathcal{F},\mathbf{r})}$.

While it is believed that the SIC-POVMs exist in every dimension, some even stronger conjectures about the existence and structure of the Weyl-Heisenberg SIC-POVMs has been stated during the last 15 years. We recall them below. Let us start from three statements, each stronger than the previous one:

[3]The Appleby's theorem is in fact more general as it covers also the case of even dimensions. Since in the thesis we consider only the case $d = 3$, we present here the simpler version of the theorem for odd dimensions.

Conjecture A (Renes et al. [**126**]). *In every dimension there exists a WH-covariant SIC-POVM.*

Conjecture B (Zauner [**168**]). *In every dimension there exists a fiducial vector for some WH-covariant SIC-POVM which is an eigenvector of the canonical order 3 unitary* $U_{\mathcal{Z}} := U_{(\mathcal{Z},0)}$*, where*

$$\mathcal{Z} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Matrix $\mathcal{Z}$ has been later referred to as the *Zauner matrix*.

Conjecture C (Appleby [**3**]). *In every dimension d there exists a fiducial vector for some WH-covariant SIC-POVM and every such vector is an eigenvector of a canonical order 3 unitary conjugated to $U_{\mathcal{Z}}$ (the conjugacy relation is considered up to a phase in the extended Clifford group).*

Grassl [**76**] gave a counter-example to the Conjecture C in dimension twelve, but there are not known counter-examples in the other dimensions. However, another conjecture by Appleby, still stronger than Conjecture A, remains open:

Conjecture D (Appleby [**3**]). *In every dimension there exists a fiducial vector for some WH-covariant SIC-POVM and every such vector is an eigenvector of a canonical order 3 unitary.*

Let us recall also that the two conjectures by Appleby are equivalent in the prime dimensions greater than three, since in these dimensions all canonical order 3 unitaries are in the same conjugacy class [**65**].

CHAPTER 3

Entropy of quantum measurement

Entropy! It's why you can't get the toothpaste back in the tube.
(Woody Allen, *Whatever works*)

The entropy of measurement is one of the tools allowing us to study the randomness of measurement outcomes, an intrinsic feature of quantum theory. In this chapter we set up the main problem of the thesis, i.e. what is the minimum value of the entropy of given measurement and what are the minimizers? We show that in the symmetric case this problem is strongly connected with computing the informational power of measurement and we give a brief insight into its relations with other problems of quantum information theory like the Wehrl entropy minimization, the entropic uncertainty principles and the quantum dynamical entropy.

3.1. Entropy

The common way to measure the uncertainty of the discrete probability distribution $P = (p_1, \ldots, p_k) \in \Delta_k := \{(p_1, \ldots, p_k) \subset [0,1]^k | \sum_{j=1}^k p_j = 1\}$ is to calculate its *Shannon entropy*[1]:

$$H(P) := \sum_{j=1}^{k} \eta(p_j), \tag{11}$$

[1]Sometimes called also the Boltzmann-Shannon entropy to emphasize the connection with the Boltzmann thermodynamic entropy. An anecdote explaining why Shannon called his function 'entropy' [**142**] exists in few versions. The first one recorded has been given by Myron Tribus [**153**], who claimed to hear it directly from Shannon himself: *When Shannon discovered this function he was faced with the need to name it for it occurred quite often in the theory of communication he was developing. He considered naming it 'information' but felt that this word had unfortunate popular interpretations that would interfere with his intended uses of it in the new theory. He was inclined towards naming it 'uncertainty' and discussed the matter with the late John Von Neumann. Von Neumann suggested that the function ought to be called 'entropy' since it was already in use in some treatises on statistical thermodynamics. Von Neumann, Shannon reports, suggested that there were two good reasons for calling the function 'entropy'. 'It is already in use under that name,' he is reported to have said, 'and besides, it will give you a great edge in debates because nobody really knows what entropy is anyway.'* However, later versions (given also by Tribus) slightly vary from this one, thus it is difficult to say how much truth is in this story, taking into account that Shannon never said a word about it and even denied in the interview with Robert Price [**121**] that he talked about it with von Neumann.

where the *Shannon entropy function* $\eta : [0,1] \to \mathbb{R}^+$ is given by $\eta(x) := -x \ln x$ for $x > 0$, and $\eta(0) := 0$. (In the sequel, we shall use frequently the identity $\eta(xy) = \eta(x) y + \eta(y) x$, for $x, y \in [0,1]$.) Obviously, H is a concave function, because η is concave.

Let $\Pi = (\Pi_j)_{j=1,\ldots,k}$ be a finite POVM in $\mathbb{C}^d$. As already mentioned in Ch. 1, the quantum measurement is nondeterministic. To be more precise, for given $\rho \in \mathcal{S}(\mathcal{H})$ the map $\{1,\ldots,k\} \ni j \mapsto p_j(\rho,\Pi) = \mathrm{Tr}(\rho\Pi_j) \in [0,1]$ defines the probability distribution of the possible measurement outcomes. We shall look for the most 'classical' or 'coherent' quantum states [2], i.e. for the states that minimize the uncertainty of the outcomes. Thus we shall minimize over $\rho \in \mathcal{S}\left(\mathbb{C}^d\right)$ the quantity called the *entropy of measurement*:

DEFINITION 3.1. By the *entropy of measurement* $H(\rho,\Pi)$ we mean the Shannon entropy of the probability distribution of the measurement outcomes, assuming that the state of the system before the measurement was ρ:

$$H(\rho,\Pi) := \sum_{j=1}^{k} \eta\left(p_j(\rho,\Pi)\right), \quad \rho \in \mathcal{S}(\mathcal{H}). \tag{12}$$

This quantity (as well as its continuous analogue) has been considered by many authors, first in the 1960s under the name of *Ingarden-Urbanik entropy* or *A-entropy*, then, since the 1980s, in the context of *entropic uncertainty principles* [**59, 101, 110, 161**], and also quite recently for more general statistical theories [**147, 144**]. Wilde called it the *Shannon entropy of POVM* [**164**]. For a history of this notion see [**162**] and [**17**].

Let us also emphasize that our approach is one of the possible answers to the question 'How much unavoidable randomness is generated by a Positive Operator Valued Measure (POVM)?', discussed in [**110**].

The function $H(\cdot,\Pi) : \mathcal{S}\left(\mathbb{C}^d\right) \to \mathbb{R}$ is continuous and concave. In consequence, it attains minima in the set of pure states. It is obviously bounded from above by $\ln k$, the entropy of the uniform distribution. The general bound from below is given in relation to the *von Neumann entropy* of the state ρ given by $S(\rho) := -\mathrm{Tr}(\rho \ln \rho)$ [**103**, Sect. 2.3]:

$$S(\rho) - \sum_{j=1}^{k} p_j \ln(\mathrm{Tr}(\Pi_j)) \le H(\rho,\Pi) \le \ln k. \tag{13}$$

Since for the normalized rank-1 POVM $\mathrm{Tr}(\Pi_j) = d/k$ for all j, we get

$$S(\rho) + \ln(k/d) \le H(\rho,\Pi) \le \ln k \tag{14}$$

and the upper bound is achieved for the maximally mixed state $\rho_* := \mathbb{I}/d$. Moreover for $\rho \in \mathcal{S}\left(\mathbb{C}^d\right)$, $S(\rho) = \min H(\rho,\Pi)$, where the minimum is taken over all

[2]The most classical with respect to a given measurement.

normalized rank-1 POVMs Π, see, e.g. [**164**, Sect. 11.1.2]. In consequence, for $\rho \in \mathcal{P}(C^d)$ we have

$$\ln(k/d) \leq H(\rho, \Pi) \leq \ln k. \tag{15}$$

The first inequality in (15) follows also from the inequalities $p_j(\rho, \Pi) \leq d/k$ for every $j = 1, \ldots, k$, see p. 19, and from the fact that ln is an increasing function.

It is sometimes much more convenient to work with the *relative entropy of measurement* (*with respect to the uniform distribution*) [**79**, p. 67] that measures non-uniformity of the distribution of the measurement outcomes and is given by

$$\widetilde{H}(\rho, \Pi) := \ln k - H(\rho, \Pi), \tag{16}$$

and to look for the states that maximize this quantity. Clearly, it follows from (14) that the relative entropy of measurement is bounded from below by 0, and from above by the *relative von Neumann entropy*[3] of the state ρ with respect to the maximally mixed state $\rho_* = \mathbb{I}/d$:

$$0 \leq \widetilde{H}(\rho, \Pi) \leq S\left(\rho || \rho_*\right) \leq \ln d. \tag{17}$$

The problem of minimizing entropy (and so maximizing relative entropy) is connected with the problem of maximization of the *mutual information* between ensembles of initial states (classical-quantum states) and the POVM Π.

Definition 3.2. Let $V = \{p_i, \tau_i\}_{i=1}^{l}$, where $p_i \geq 0$ are *a priori* probabilities of density matrices $\tau_i \in \mathcal{S}\left(\mathbb{C}^d\right)$, where $i = 1, \ldots, l$, and $\sum_{i=1}^{l} p_i = 1$. The *mutual information* between V and Π is given by:

$$I(V, \Pi) := I(P) := \sum_{i=1}^{l} \eta\left(\sum_{j=1}^{k} P_{ij}\right) + \sum_{j=1}^{k} \eta\left(\sum_{i=1}^{l} P_{ij}\right) - \sum_{i=1}^{l}\sum_{j=1}^{k} \eta(P_{ij}), \tag{18}$$

where $P_{ij} := p_i \mathrm{Tr}\left(\tau_i \Pi_j\right)$ for $i = 1, \ldots, l$ and $j = 1, \ldots, k$.

The problem of maximization of $I(V, \Pi)$ consists of two dual aspects [**12, 89, 91**]: maximization over all possible measurements, providing the ensemble V is given, see, e.g. [**87, 53, 135, 151**], and (less explored) maximization over ensembles, when the POVM Π is fixed [**11, 117**]. In the former case, the maximum is called *accessible information*. In the latter case, Dall'Arno et al. [**11, 12**] introduced the name *informational power of* Π for the maximum and denoted it by $W(\Pi)$. Oreshkov et al. showed that there exists a *maximally informative ensemble* (i.e. ensemble that maximizes the mutual information) consisting of pure states only [**117**].

Note that a POVM Π generates a *quantum-classical channel* $\Phi : \mathcal{S}\left(\mathbb{C}^d\right) \to \mathcal{S}\left(\mathbb{C}^k\right)$ given by $\Phi(\rho) = \sum_{j=1}^{k} \mathrm{tr}\left(\rho \Pi_j\right) |e_j\rangle \langle e_j|$, where $\left(|e_j\rangle\right)_{j=1}^{k}$ is any orthonormal basis in $\mathbb{C}^k$. The *minimum output entropy* of Φ is equal to the minimum entropy of Π, i.e. $\min_\rho S(\Phi(\rho)) = \min_\rho H(\rho, \Pi)$ [**143**]. Moreover, the informational power

[3] $S(\rho||\sigma) := \mathrm{Tr}(\rho(\ln \rho - \ln \sigma))$

of Π can be identified [**90, 117**] as the *classical capacity* $\chi(\Phi)$ of the channel Φ, i.e.

$$W(\Pi) = \chi(\Phi) := \max_{V=\{p_i,\tau_i\}} \left\{ S\left(\sum_i p_i \Phi(\rho_i)\right) - \sum_i p_i S(\Phi(\rho_i)) \right\}.$$

We shall compute its value for all HS-POVMs in dimension two, as well as for SIC-POVMs in dimension three, in Sect. 4.7.

3.2. Entropy in symmetric case

Let us consider a POVM Π that is G-covariant (or, in case of rank-1 POVM, symmetric; then G can be identified with $\mathrm{Sym}(S)$, where S is a set of pure states corresponding to Π). It is a simple observation that both the relative entropy of Π and the mutual information do not depend on whether Π is defined to be a set or multiset, and so for the convenience we assume the latter one. Oreshkov et al. [**117**] proved for such POVM the existence of a maximally informative ensemble consisting of equiprobable elements of the orbit of a pure state under the action generated by the dual representation of G. Note that for every such ensemble of the form $V(\rho) := \{1/|G|, \sigma_g^*(\rho)\}_{g\in G}$, where $\rho \in \mathcal{S}(\mathcal{H})$ we have

$$P_{gh} = \frac{1}{|G|}\mathrm{Tr}\left(\sigma_g^*(\rho)\Pi_h\right) = \frac{1}{|G|}\mathrm{Tr}\left(\rho\sigma_g(\Pi_h)\right) \tag{19}$$

and so

$$\sum_{h\in G} P_{gh} = \sum_{g\in G} P_{gh} = \frac{1}{|G|}. \tag{20}$$

In consequence we get after simple calculation

$$I(V(\rho), \Pi) = \widetilde{H}(\rho, \Pi). \tag{21}$$

Hence, these two maximization problems: of the relative entropy over mixed or pure states and of the mutual information over ensembles are equivalent in this case, i.e.

$$W(\Pi) = \max_{V\text{-ensemble}} I(V, \Pi) = \max_{\rho\in\mathcal{S}(\mathbb{C}^d)} \widetilde{H}(\rho, \Pi) = \max_{\rho\in\mathcal{P}(\mathbb{C}^d)} \widetilde{H}(\rho, \Pi). \tag{22}$$

Note, however, that there may exist a maximally informative ensemble that is not G-covariant, see, e.g. [**11**, Prop. 9].

Let now $\Pi = (\Pi_j)_{j=1,\dots,k}$ be a finite normalized rank-1 POVM in $\mathbb{C}^d$ and $S := \{\rho_j : j = 1, \dots, k\}$ be a corresponding (multi-)set of pure quantum states, i.e. $\rho_j \in \mathcal{P}(\mathbb{C}^d)$ and $\Pi_j = (d/k)\,\rho_j$ for $j = 1, \dots, k$. Then we get after simple calculations

$$H(\rho, \Pi) = \frac{d}{k}\sum_{j=1}^{k} \eta\left(\mathrm{Tr}\left(\rho\rho_j\right)\right) - \ln\left(d/k\right) \tag{23}$$

and so

$$\widetilde{H}(\rho,\Pi) = \ln d - \frac{d}{k}\sum_{j=1}^{k}\eta\left(\mathrm{Tr}\left(\rho\rho_j\right)\right) \tag{24}$$

for $\rho \in \mathcal{P}(\mathbb{C}^d)$. Assume now, that Π is symmetric (group covariant) and put $G := \mathrm{Sym}\,(S)$. Then for each $\tau \in S$ we have $S = \{g\tau : g \in G\}$ and

$$\begin{aligned}\widetilde{H}(\rho,\Pi) &= \ln d - \frac{d}{|G|}\sum_{g\in G}\eta\left(\mathrm{Tr}\left(\rho\left(g\tau\right)\right)\right) \\ &= \ln d - \frac{d}{|S|}\sum_{[g]\in G/G_\tau}\eta\left(\mathrm{Tr}\left(\rho\left(g\tau\right)\right)\right)\end{aligned} \tag{25}$$

for $\rho \in \mathcal{P}(\mathbb{C}^d)$. The same formulae are true for any subgroup of $\mathrm{Sym}\,(S)$ acting transitively on S. Note that the behaviour of the functions $H(\cdot,\Pi)$, $\widetilde{H}(\cdot,\Pi) : \mathcal{P}(\mathbb{C}^d) \to \mathbb{R}^+$ depends only on the choice of the fiducial state τ. Moreover, observe that both functions are G-invariant, as for $\rho \in \mathcal{P}(\mathbb{C}^d)$ and $g \in G$ we have $\mathrm{Tr}(\rho(g\tau)) = \mathrm{Tr}(\tau(g^{-1}\rho))$, and so from (25) we get

$$H(\rho,\Pi) = \frac{d}{|G|}\sum_{g\in G}\eta\left(\mathrm{Tr}\left(\tau\left(g\rho\right)\right)\right) - \ln(d/k) \tag{26}$$

and

$$\widetilde{H}(\rho,\Pi) = \ln d - \frac{d}{|G|}\sum_{g\in G}\eta\left(\mathrm{Tr}\left(\tau\left(g\rho\right)\right)\right). \tag{27}$$

3.3. Relation to Wehrl entropy minimization

The relative entropy of symmetric POVM is closely related to the semi-classical quantum entropy introduced in 1978 by Wehrl for the harmonic oscillator coherent states [**162**] and named later after him. The definition was generalised by Schroeck [**136**], who analysed its basic properties. Let G be a compact topological group acting unitarily and irreducibly on $\mathcal{P}\left(\mathbb{C}^d\right)$. Fixing fiducial state $\tau \in \mathcal{P}\left(\mathbb{C}^d\right)$ we get the family of states $(g\tau)_{g\in G/G_\tau}$ called (*generalized* or *group*) *coherent states* [**120, 1**] that fulfills the identity: $\int_{G/G_\tau} g\tau d\mu([g]_{G/G_\tau}) = \mathbb{I}$, where μ is the G-invariant measure on G/G_τ such that $\mu\left(G/G_\tau\right) = d$. Then for $\rho \in \mathcal{S}\left(\mathbb{C}^d\right)$ we define the *generalized Wehrl entropy* of ρ by

$$S_{Wehrl}\left(\rho\right) := \int_{G/G_\tau}\eta\left(\mathrm{tr}\left(\rho\left(g\tau\right)\right)\right)d\mu([g]_{G/G_\tau}). \tag{28}$$

It is just the Boltzmann-Gibbs entropy[4] for the density function on $(G/G_\tau,\mu)$ called the *Husimi function* of ρ and given by $G/G_\tau \ni [g]_{G/G_\tau} \to \mathrm{tr}\left(\rho\left(g\tau\right)\right) \in \mathbb{R}^+$ that represents the probability density of the results of an approximate coherent states measurement (or in other words continuous POVM) [**52, 36**]. Then the relative Boltzmann-Gibbs entropy of the Husimi distribution of ρ with respect

[4]The continuous analogue of the Shannon entropy.

to the Husimi distribution of the maximally mixed state ρ_*, that is the constant density on $(G/G_\tau, \mu)$ equal $1/d$, given by

$$S_{Wehrl}(\rho|\rho_*) := \ln d - S_{Wehrl}(\rho) \tag{29}$$

is a continuous analogue of $\widetilde{H}(\cdot, \Pi)$ given by (25). What is more, the relative entropy of measurement is just a special case of such transformed Wehrl entropy, when we consider the discrete coherent states (i.e. POVM) generated by a finite group. On the other hand, the entropy of measurement $H(\cdot, \Pi)$ has no continuous analogue, as it may diverge to infinity, where $k \to \infty$. In principle, to define coherent states we can use an arbitrary fiducial state. However, to obtain coherent states with sensible properties one has to choose the fiducial state τ to be the *vacuum state*, that is the state with maximal symmetry with respect to G [**100**],[**120**, Sect. 2.4].

To investigate the Wehrl entropy it is enough to require that G should be locally compact. In fact, Wehrl defined this quantity for the *harmonic oscillator coherent states*, where G is the Heisenberg-Weyl group H_4 acting on projective (infinite dimensional and separable) Hilbert space, $G_\tau \simeq U(1) \times U(1)$, and $G/G_\tau \simeq \mathbb{C}$. This notion was generalized by Lieb [**105**] to *spin* (*Bloch*) *coherent states*, with $G = SU(2)$ acting on $\mathbb{CP}^{d-1}$ ($d \geq 2$), $G_\tau \simeq U(1)$ and $G/G_\tau \simeq S^2$. In this paper Lieb proved that for harmonic oscillator coherent states the minimum value of the Wehrl entropy is attained for coherent states themselves. (It follows from the group invariance that this quantity is the same for each coherent state.) He also conjectured that the statement is true for spin coherent states, but, despite many partial results, the problem, called the *Lieb conjecture*, had remained open for next thirty five years until it was finally proved by Lieb himself and by Solovej in 2012 [**106**]. They also expressed the hope that the same result holds for $SU(N)$ coherent states for arbitrary $N \in \mathbb{N}$, or even for any compact connected semisimple Lie group (the *generalized Lieb conjecture*), see also [**72, 147**]. Bandyopadhyay received recently some partial results in this direction for $G = SU(1,1)$ coherent states [**18**], where $G_\tau \simeq U(1)$ and G/G_τ is the hyperbolic plane.

For finite groups and covariant POVMs the minimization of Wehrl entropy is equivalent to the maximization of the relative entropy of measurement, which is in turn equivalent to the minimization of the entropy of measurement. Consequently, one could expect that the entropy of measurement should be minimal for the states constituting the POVM that are already known to be critical as inert states, see p. 44. We shall see in Sect. 4.3 that this need not be always the case. In particular, it is not true for SIC-POVMs, as well as in dimension two where the Bloch vectors of the states constituting a POVM form a regular polygon with odd number of vertices. Thus, it is conceivable that to prove the 'generalized Lieb conjecture' some additional assumptions will be necessary.

3.4. Entropic uncertainty relations

The entropic uncertainty principles form another area of research related to quantifying the uncertainty in quantum theory. They were introduced by Białynicki-Birula and Mycielski [**27**], who showed that they are stronger than 'standard' Heisenberg's uncertainty principle, and Deutsch [**59**], who provided the first lower bound for the sum of entropic uncertainties of two observables independent on the initial state. This bound has been later improved by Maassen and Uffink [**108, 155**], and de Vicente and Sánchez-Ruiz [**157**]. The generalizations for POVMs (all previous results referred to PVMs) has been provided subsequently in [**81, 101, 110**] and [**124**]. More detailed survey of the topic can be found in [**161**].

The entropic uncertainty relations are closely connected with entropy minimization. In fact, any lower bound for the entropy of measurement can be regarded as an *entropic uncertainty relation for single measurement* [**101**]. Moreover, combining m normalized rank-1 POVMs $\Pi^i = (\Pi^i_j)_{j=1,\dots,k_i}$ $(i = 1,\dots,m)$ we obtain another normalized rank-1 POVM $\Pi := (\frac{1}{m}\Pi^i_j)^{i=1,\dots,m}_{j=1,\dots,k_i}$. Now, from an entropic uncertainty principle for $(\Pi^i)_{i=1,\dots,m}$ written in the form $\frac{1}{m}\sum_{i=1}^m H(\rho,\Pi^i) \geq C > 0$ [**161**, p. 3] we get automatically a lower bound for entropy of Π, namely

$$H(\rho,\Pi) = \frac{1}{m}\sum_{i=1}^{m} H(\rho,\Pi^i) + \ln m \geq C + \ln m \tag{30}$$

for $\rho \in \mathcal{P}\left(\mathbb{C}^d\right)$, and vice versa, proving a lower bound for entropy of Π we get immediately an entropic uncertainty principle.

To be more specific, assume now that $m = 2$ and $\Pi^i_j = (d/k)\,\rho^i_j$, where $\rho^i_j = \left|\varphi^i_j\right\rangle\left\langle\varphi^i_j\right| \in \mathcal{P}\left(\mathbb{C}^d\right)$, denoting their Bloch vectors by $x^i_j := b\left(\rho^i_j\right) \in \mathcal{L}^0_s(\mathbb{C}^d) \simeq \mathbb{R}^{d^2-1}$ for $j = 1,\dots,k$, $i = 1,2$. The *Krishna-Parthasarathy entropic uncertainty principle* [**101**, Corol. 2.6], combined with (5) and (30) gives us

$$\begin{aligned} H(\rho,\Pi) &\geq \ln(2k/d) - \ln \max_{j,l=1,\dots,k} \left|\left\langle\varphi^1_j|\varphi^2_l\right\rangle\right| \\ &= \ln(2k/d) - \frac{1}{2}\ln(\max_{j,l=1,\dots,k} \left\langle\left\langle x^1_j, x^2_l\right\rangle\right\rangle_{HS} + 1/d) \end{aligned} \tag{31}$$

for $\rho \in \mathcal{P}\left(\mathbb{C}^d\right)$. In consequence, taking into account that the radius of the Bloch sphere is $\sqrt{1-1/d}$, we get an upper bound for relative entropy

$$\begin{aligned} \widetilde{H}(\rho,\Pi) &\leq \ln d + \frac{1}{2}\ln(\max_{j,l=1,\dots,k} \left\langle\left\langle x^1_j, x^2_l\right\rangle\right\rangle_{HS} + 1/d) \\ &= \ln d + \frac{1}{2}\ln((1-1/d)(\max_{j,l=1,\dots,k}\cos(2\theta_{jl})) + 1/d)), \end{aligned} \tag{32}$$

where $\theta_{jl} := \measuredangle\left(x^1_j, x^2_l\right)/2$ for $j,l = 1,\dots,k$. As this upper bound does not depend on the input state ρ, it gives us also an upper bound for the informational power of Π.

If $d = 2$, this inequality takes a simple form

$$\widetilde{H}(\rho, \Pi) \leq \ln 2 + \ln \max_{j,l=1,\ldots,k} |\cos \theta_{jl}| . \tag{33}$$

We may used this bound, e.g. for the 'rectangle' POVM analysed in Sect. 4.2, that can be treated as the aggregation of two pairs of antipodal points on the sphere representing two PVM measurements. In this case we deduce from (33) that $\widetilde{H} \leq \ln 2 + \ln \max (|\sin (\alpha/2)| , |\cos (\alpha/2)|)$, where α is the measure of the angle between the diagonals of the rectangle. In particular, for the 'square' POVM we get $\widetilde{H} \leq \frac{1}{2} \ln 2$. As we shall see in Sect. 4.7, this bound is actually reached for each of four states constituting the POVM and represented by the vertices of the square.

3.5. Relation to quantum dynamical entropy

As in the preceding section, let $\Pi = (\Pi_j)_{j=1,\ldots,k}$ be a finite normalized rank-1 POVM in $\mathbb{C}^d$ and let $S = \{\rho_j : j = 1, \ldots, k\}$ be a corresponding (multi-)set of pure quantum states. Set $\rho_j = |\varphi_j\rangle \langle\varphi_j|$, where $\varphi_j \in \mathbb{C}^d$, $\|\varphi_j\| = 1$. Assume that successive measurements described by the generalized Lüders instrument connected with Π, where ρ_i serve as the 'output states', are performed on an evolving quantum system and that the motion of the system between two subsequent measurements is governed by a unitary matrix U. Clearly, the sequence of measurements introduces a nonunitary evolution and the complete dynamics of the system can be described by a quantum Markovian stochastic process, see [**145**].

The results of consecutive measurements are represented by finite strings of letters from a k-element alphabet. Probability of obtaining the string $(i_1, \ldots, i_n)$, where $i_j = 1, \ldots, k$ for $j = 1, \ldots, n$ and $n \in \mathbb{N}$ is then given by

$$P_{i_1,\ldots,i_n}(\rho) := p_{i_1}(\rho) \cdot \prod_{m=1}^{n-1} p_{i_m i_{m+1}}, \tag{34}$$

where ρ is the initial state of the system, $p_i(\rho) := (d/k) \operatorname{tr}(\rho\rho_i)$ is the probability of obtaining i in the first measurement, and $p_{ij} := (d/k) \operatorname{tr}(U\rho_i U^* \rho_j) = (d/k) |\langle\varphi_i|U|\varphi_j\rangle|^2$ is the probability of getting j as the result of the measurement, providing the result of the preceding measurement was i, for $i, j = 1, \ldots, k$ [**145, 147**]. The randomness of the measurement outcomes can be analysed with the help of (*quantum*) *dynamical entropy*, the quantity introduced for the Lüders-von Neumann measurement independently by Srinivas [**149**], Pechukas [**119**], Beck & Graudenz [**21**] and many others, see [**145**, p. 5685], then generalized by Słomczyński and Życzkowski to arbitrary classical or quantum measurements and instruments [**145, 102, 146, 147**], and recently rediscovered by Crutchfield and Wiesner under the name of *quantum entropy rate* [**48**].

The definition of (*quantum*) *dynamical entropy of U with respect to* Π mimics its classical counterpart, the Kolmogorov-Sinai entropy:

$$H(U,\Pi) := \lim_{n\to\infty}(H_{n+1}-H_n) = \lim_{n\to\infty} H_n/n, \tag{35}$$

where $H_n := \sum_{i_1,\ldots,i_n=1}^{k} \eta\left(P_{i_1,\ldots,i_n}(\rho_*)\right)$ for $n \in \mathbb{N}$. The maximally mixed state $\rho_* = \mathbb{I}/d$ plays here the role of the 'stationary state' for combined evolution. It is easy to show that the quantity is given by

$$\begin{aligned} H(U,\Pi) &= \frac{1}{k}\sum_{i,j=1}^{k} \eta\left((d/k)\operatorname{tr}(U\rho_i U^* \rho_j)\right) \\ &= \ln(k/d) + \frac{d}{k^2}\sum_{i,j=1}^{k} \eta\left(\operatorname{tr}(U\rho_i U^*\rho_j)\right) \\ &= \ln(k/d) + \frac{d}{k^2}\sum_{i,j=1}^{k} \eta\left(|\langle\varphi_i|U|\varphi_j\rangle|^2\right), \end{aligned} \tag{36}$$

which is a special case of much more general integral entropy formula [**147**]. Using (23) and (36) we see that the dynamical entropy of U is expressed as the mean entropy of measurement over output states transformed by U:

$$H(U,\Pi) = \frac{1}{k}\sum_{i=1}^{k} H(U\rho_i U^*, \Pi) \tag{37}$$

There are two sources of randomness in this model: the underlying unitary dynamics and the measurement process. The latter can be measured by the quantity $H_{meas}(\Pi) := H(\mathbb{I},\Pi)$ called *(quantum) measurement entropy*. From (37) we get

$$H_{meas}(\Pi) = \frac{1}{k}\sum_{i=1}^{k} H(\rho_i,\Pi). \tag{38}$$

If Π is symmetric, then all the summands in (38) are the same. Hence, in this case, the measurement entropy $H_{meas}(\Pi)$ is equal to the entropy of measurement $H(\rho,\Pi)$, where the input state ρ is one of the output states from S.

3.6. Majorization and generalized entropies

Although the Shannon entropy is the most commonly used measure of uncertainty, mainly due to the wide range of distinctive properties, one can consider also other entropy-like functions defined on the probability simplex Δ_k. Among the desirable features of such generalized entropy one should expect the function to be maximal for the uniform distribution and minimal when there is no randomness, i.e. all but one coefficients are equal 0. It should be also invariant under permutations. However, while the Shannon entropy is concave, we would slightly loosen this demand for the generalized entropy.

A concept strongly connected with the convexity (or concavity) is a preorder defined on $\mathbb{R}^k$ called *majorization* (the theory in its most complete shape is gathered in [**109**]). We say that $u \in \mathbb{R}^k$ *majorizes* $v \in \mathbb{R}^k$ and denote it by $u \succ v$, if $\sum_{i=1}^{s} u_i^{\downarrow} \geq \sum_{i=1}^{s} v_i^{\downarrow}$ for all $s = 1, \ldots, k-1$, and $\sum_{i=1}^{k} u_i^{\downarrow} = \sum_{i=1}^{k} v_i^{\downarrow}$, where by $u_i^{\downarrow}$ and $v_i^{\downarrow}$ we denote the coordinates of u and v ordered decreasingly. A function $F : \mathbb{R}^k \supset A \to \mathbb{R}$ is said to be *Schur-convex* (resp. *Schur-concave*) on A if for every $u, v \in A$ such that $u \succ v$ we have $F(u) \geq F(v)$ (resp. $F(u) \leq F(v)$). In particular, every convex (resp. concave) function on $A \subset \mathbb{R}^k$ that is *symmetric*, i.e. invariant under permutations of the coordinates is Schur-convex (resp. Schur-concave) [**109**, Prop. 3.C.2]. Thus, the Shannon entropy is also an example of a Schur-concave function on Δ_k. A function $F : \mathbb{R}^k \supset A \to \mathbb{R}$ is said to be *strictly Schur-convex* (resp. *strictly Schur-concave*) on A if it is Schur-convex (resp. Schur-concave) and $F(u) > F(v)$ (resp. $F(u) < F(v)$) for every $u, v \in A$ such that $u \succ v$ and u is not a permutation of v.

Following [**24**], we define a *generalized entropy* to be any function $F : \Delta_k \to \mathbb{R}$ that is Schur-concave on Δ_k.[5] Below we give examples of two families of such function, both of them containing the Shannon entropy as a special case:

Example 3.1 (Havrda-Charvát-Tsallis α-entropy [**83, 154**]). Let us consider a function given by $\theta_\alpha(t) := (t - t^\alpha)/(\alpha - 1)$ for $0 \leq t \leq 1$, where $0 < \alpha \neq 1$. It is concave and fulfills $\lim_{\alpha \to 1} \theta_\alpha = \eta$. Now, let $H_\alpha : \Delta_k \to \mathbb{R}$ be defined by $H_\alpha(p_1, \ldots, p_k) := \sum_{j=1}^{k} \theta_\alpha(p_j)$ for $p \in \Delta_k$. It is obviously concave and symmetric, and thus it is also Schur-concave. H_α is called *Havrda-Charvát-Tsallis α-entropy*[6] and, in particular, for $\alpha = 2$, *linear entropy* [**24, 49**]. In the limit $\alpha \to 1$ we get the Shannon entropy. ■

Example 3.2 (Rényi α-entropy [**127**]). The *Rényi α-entropy* can be obtained by composing function g_α given by $g_\alpha(x) = (1-\alpha)^{-1} \ln((1-\alpha)x + 1)$ with H_α, i.e. $R_\alpha : \Delta_k \to \mathbb{R}$ is defined by $R_\alpha(p_1, \ldots, p_k) = g_\alpha(H_\alpha(p_1, \ldots, p_k)) = (1-\alpha)^{-1} \ln\left(\sum_{j=1}^{k} p_j^\alpha\right)$ for $p \in \Delta_k$ and $0 < \alpha \neq 1$. Note that again we get the Shannon entropy as $\alpha \to 1$. This function does not need necessarily to be concave (see, e.g. [**24**, Ch. 2.7]), however, by Schur's theorem, it is still Schur-concave. ■

The Havrda-Charvát-Tsallis α-entropy of POVM and the Rényi α-entropy of POVM can be defined in the same way as was the (Shannon) entropy of measurement. Recently both of them has been studied by Rastegin [**125**] in the

[5] However, some would require more restrictive definition, in order to guarantee certain desired properties such as the uniqueness of minimizer and maximizer (up to permutation) or some kind of continuity. One of the ideas (communicated privately) comes from Grzegorz Harańczyk who claims that reasonable definition of generalized entropy could be a function which is strictly Schur-concave and lower semicontinuous.

[6] To be more precise, H_α denotes Tsallis α-entropy, while the α-entropy introduced by Havrda and Charvát differs from it by a constant factor.

context of entropic uncertainty relations for mutually unbiased bases (MUBs) and single SIC-POVMs. We will see in Secs 4.3.2 and 4.4 that his lower bounds for SIC-POVMs are satisfied in dimensions two and three.

Note that since tight informationally complete POVMs (e.g. informationally complete HS-POVMs in dimension two or SIC-POVMs in any dimension) are complex projective 2-designs (Proposition 2.3), so the linear entropy H_2 (and so R_2) is constant, i.e. independent on the choice of the input state. Moreover, it follows from Remark 2.2 that the entropy H_3 (and so R_3) is constant for HS-POVMs in dimension two with octahedral symmetry, and the entropies H_3, H_4 and H_5 (and so R_3, R_4 and R_5) are constant for HS-POVMs in dimension two with icosahedral symmetry.

CHAPTER 4

Results

'But look, the King's still standing!'
'Still standing, eh? Factor both sides, divide by two, throw in a few imaginary numbers – good! Now change variables and subtract – Trurl, what on earth are you doing?! The beast, not the King, the beast! That's right! Good! Perfect!! Now transform, approximate and solve for x. Do you have it?'
'I have it! Klapaucius! Look at the King now!!'
There was a pause, then a burst of wild laughter.

(Stanisław Lem, *The Cyberiad*)

Before we present the main results of the thesis, we describe the methods used in the proofs, including Michel theory of critical orbits of group invariant functions and the minimization method based on the Hermite interpolation, and provide the necessary tools as group invariant polynomials. We reveal also why the majorization technique is not useful in the general approach. We start presenting the results with a characterization of the critical orbits of the entropy of measurement for highly symmetric POVMs in dimension two that arise from the group-invariance. Next we give a proof that the local minimizers found in this way are in fact global. Then we provide a characterization of minimizers for SIC-POVMs in dimension three in both algebraic and geometric terms. Afterwards we discuss the problem of finding the pure states of maximal entropy, giving exact solutions for HS-POVMs in dimension two and SIC-POVMs in any dimension. We conclude with providing the formula for the average value of the relative entropy and comparing it with the informational power of POVMs for which we were able to calculate it.

4.1. General methods

4.1.1. Entropy in the Bloch representation. Using the Bloch representation for states and normalized rank-1 POVMs (see Sect. 1.3) one can present the problems of entropy minimization and relative entropy maximization as the problem of finding the global extrema of the corresponding function on $B(d) \subset S^{d^2-2}$. Such reformulation significantly reduces the complexity of the problem in dimension two, since then $B(2) = S^2$. Let $\Pi = (\Pi_j)_{j=1,\ldots,k}$ be a normalized rank-1 POVM in $\mathbb{C}^d$ such that $\Pi_j = (d/k)\,\rho_j$, $\rho_j \in \mathcal{P}\left(\mathbb{C}^d\right)$, and let

$B := \{v_j | j = 1, \ldots, k\}$, where $v_j := (1/\sqrt{d-1})\vec{b}_{\rho_j} \in S^{d^2-2}$ $(j = 1, \ldots, k)$. For $\rho \in \mathcal{P}\left(\mathbb{C}^d\right)$, $u := (1/\sqrt{d-1})\vec{b}_\rho \in S^{d^2-2}$ and $j = 1, \ldots, k$ we get from (8)

$$p_j(\rho, \Pi) = ((d-1)u \cdot v_j + 1)/k. \tag{39}$$

Applying (39), (23) and (24) we obtain

$$H_B(u) := H(\rho, \Pi) = \sum_{j=1}^{k} \eta\left(\frac{(d-1)u \cdot v_j + 1}{k}\right) = \ln\frac{k}{d} + \frac{d}{k}\sum_{j=1}^{k} h\left(u \cdot v_j\right) \tag{40}$$

and

$$\widetilde{H}_B(u) := \widetilde{H}(\rho, \Pi) = \ln d - \frac{d}{k}\sum_{j=1}^{k} h\left(u \cdot v_j\right), \tag{41}$$

where the function $h : [-1/(d-1), 1] \to \mathbb{R}^+$ is given by

$$h\left(t\right) := \eta\left(\frac{(d-1)t + 1}{d}\right) \tag{42}$$

for $-1 \leq t \leq 1$. It is clear that the functions H_B and $\widetilde{H}_B : B(d) \to \mathbb{R}^+$ are of C^2 class (even analytic) except at the points 'orthogonal' to the points from B (in the sense that they represent orthogonal states to states ρ_j, $j = 1, \ldots, k$). Despite the fact that the function h is non-differentiable at $-1/(d-1)$, some standard calculations show that, e.g. in dimension two the functions H_B and $\widetilde{H}_B$ are of C^1 class; however, they are not twice differentiable.

For a symmetric POVM, there exists a finite group $G \subset O\left(d^2-1\right)$ acting transitively on B. It follows from (40) and (41) that H_B and $\widetilde{H}_B$ are G-invariant functions on $B(d)$ given by

$$H_v(u) := H_B(u) = \ln\frac{|G|}{d} + \frac{d}{|G|}\sum_{g \in G} h\left(gu \cdot v\right) \tag{43}$$

and

$$\widetilde{H}_v(u) := \widetilde{H}_B(u) = \ln d - \frac{d}{|G|}\sum_{g \in G} h\left(gu \cdot v\right), \tag{44}$$

for $u \in B(d)$, where $v \in B = \{gv : g \in G\}$ is the normalized Bloch vector of an arbitrary fiducial state. This fact allows us to use the theory of solving symmetric variational problems developed by Louis Michel and others in the 1970s, and applied since then in many physical contexts, especially in analysing the spontaneous symmetry breaking phenomenon [**113**].

4.1.2. Michel theory. We start by quoting several theorems concerning smooth action of finite groups on finite-dimensional manifolds. They are usually formulated for compact Lie groups, but since finite groups are zero-dimensional Lie group, thus the results apply equally well in this case.

Let G be a finite group of C^1 maps acting on a compact finite-dimensional manifold M. In the set of strata consider the order $\prec$ introduced in Sect. 2.1. Then

THEOREM (Montgomery and Yang [**114**, Thm 4a], [**115, 64**]). *The set of strata is finite. There exists a unique minimal stratum, comprising elements of trivial stabilizers, that is open and dense in M, called* ***generic*** *or* ***principal****. For every $x \in M$ the set $\bigcup\{\Sigma_u : u \in M,\ \Sigma_x \preceq \Sigma_u\}$ is closed in M; in particular, the maximal strata are closed.*

The next result tells us, where we should look for the critical points of an invariant function, i.e. the points where its gradient vanishes: we have to focus on the maximal stratum of G action on M.

THEOREM (Michel [**114**, Corol. 4.3], [**112**]). *Let $F : M \to \mathbb{R}$ be a G-invariant C^1 map, and let Σ be a maximal stratum. Then*

(1) Σ contains some critical points of F;

(2) if Σ is finite, then all its elements are critical points of F.

Such points are called *inert states* in physical literature; they are critical regardless of the exact form of F, see, e.g. [**165**]. Of course, an invariant function can have other critical points than those guaranteed by the above theorem (*non-inert states*). However, we shall see that for highly symmetric POVMs in dimension two, the global minima of entropy function H_B lie always on maximal strata. Although Michel's theorem indicates a special character of the points with maximal stabilizer, it does not give us any information about the nature of these critical points. In some cases we can apply the following result:

THEOREM (Modern Purkiss Principle [**160**, p. 385]). *Let $F : M \to \mathbb{R}$ be a G-invariant C^2 map and let $u \in M$. Assume that the action of the linear isotropy group $\{T_u h : h \in G_u\}$ on $T_u M$ is irreducible. Then u is a critical point of F, which is either degenerate (i.e. the Hessian of F is singular at u) or a local extremum of F.*

4.1.3. The minimization method based on the Hermite interpolation. The entropy function seems to be too complicated to solve the minimization problem directly. Thus the main purpose of the method presented here is to simplify the problem in such a way that we will need to deal with polynomials instead of entropy itself.

Let us recall how the Hermite interpolation works. Consider a sequence of points $a \le t_1 < t_2 < \ldots < t_m \le b$, a sequence of positive integers $k_1, k_2, \ldots, k_m$, and a real valued function $f \in C^D([a,b])$, where $D := k_1 + k_2 + \ldots + k_m$.[1] We

[1]In fact it is enough to assume less. For our purposes it suffices that f is continuous, $f \in C^D((a,b))$ and, if $t_1 = a$ or $t_m = b$, the one-sided derivatives in a and b are of order $k_1 - 1$

are looking for a polynomial p of degree less than D that agree with f at t_i up to a derivative of order $k_i - 1$ (for $1 \le i \le m$), that is,

$$p^{(k)}(t_i) = f^{(k)}(t_i), \qquad 0 \le k < k_i. \tag{45}$$

The existence and uniqueness of such polynomial follows from the injectivity (and hence also the surjectivity) of a linear map $\Phi : \mathbb{R}_{<D}[X] \to \mathbb{R}^D$ given by $\Phi(p) := (p(t_1), p'(t_1), \ldots, p^{(k_1-1)}(t_1), \ldots, p(t_m), \ldots, p^{(k_m-1)}(t_m))$. We will also use the following well-known formula for the error in Hermite interpolation [**150**, Sect. 2.1.5]:

Lemma 4.1. *For each $t \in (a,b)$ there exists $\xi \in (a,b)$ such that* $\min\{t, t_1\} < \xi < \max\{t, t_m\}$ *and*

$$f(t) - p(t) = \frac{f^{(D)}(\xi)}{D!} \prod_{i=1}^{m} (t - t_i)^{k_i}. \tag{46}$$

Now we put some constraints on function f, namely we assume that all its derivatives of even order are strictly negative in (a,b) and these of odd order greater than 1 are strictly positive:

$$f^{2l}(x) < 0, \quad f^{2l+1}(x) > 0 \quad \text{for } x \in (a,b),\ l = 1, 2, \ldots. \tag{47}$$

Moreover, let us assume that

$$k_i := \begin{cases} 1, & \text{if } t_i \in \{a, b\} \\ 2, & \text{otherwise} \end{cases}. \tag{48}$$

Observation 4.2. *Under above assumptions we get that the Hermite polynomial p interpolates f*

(1) from below, if $t_1 = a$,
(2) from above, if $t_1 > a$.

Moreover, $f(t) = p(t)$ if and only if $t = t_i$ for some $i = 1, \ldots, m$.

Proof. (1) We consider two cases: when $t_m = b$ and when $t_m < b$. In the first one we have $D = 2m - 2$, so $f^{(D)}(\xi) < 0$ for $\xi \in (a,b)$. We also get

$$\prod_{i=1}^{m} (t - t_i)^{k_i} = (t-a)(t-b) \prod_{i=2}^{m-1} (t - t_i)^2 \le 0, \tag{49}$$

for $t \in [a,b]$. Similarly, in the second case we have $D = 2m - 1$ and so $f^{(D)}(\xi) > 0$ for $\xi \in (a,b)$. Moreover,

$$\prod_{i=1}^{m} (t - t_i)^{k_i} = (t-a) \prod_{i=2}^{m} (t - t_i)^2 \ge 0 \tag{50}$$

and $k_m - 1$, respectively. In particular, it shall enable us to use Lemma 4.1, since its proof involves applying Roll's theorem an adequate number of times to an appropriate function.

for $t \in [a,b]$. Finally, we apply (46) to get $f(t) \geq p(t)$ for $t \in [a,b]$ with equality exactly in the points t_i for $i = 1, \ldots, m$. The proof of (2) is analogous. $\square$

How can we apply this method in our situation or even in more general setting of generalized entropies? For $B = \{v_j | j = 1, \ldots, k\} \subset B(d)$ we define $F : B(d) \to \mathbb{R}$ by $F(u) := \hat{g}(\sum_{j=1}^{k} f(u \cdot v_j))$, where $\hat{g} : \mathbb{R} \to \mathbb{R}$ is strictly increasing and $f : [-1/(d-1), 1] \to \mathbb{R}$ fulfills the condition given in (47). (In case of Shannon entropy $f = h$ given by (42) and $\hat{g}$ is the identity.) For the set of the interpolation points we take $T := \{w \cdot v_j | j = 1, \ldots, k\}$, where $w \in B(d)$. Then, by Observation 4.2, if $-1/(d-1) \in T$, we get for every $u \in B(d)$

$$F(u) = \hat{g}\left(\sum_{j=1}^{k} f(u \cdot v_j)\right) \geq \hat{g}\left(\sum_{j=1}^{k} p(u \cdot v_j)\right) =: P(u) \tag{51}$$

with equality for $u = w$ (and any other u satisfying $\{u \cdot v_j | j = 1, \ldots, k\} \subset T$). Similarly, if $-1/(d-1) \notin T$ we get $F(u) \leq P(u)$ with equality for u as above.

Note that if B is a set of normalized Bloch vectors corresponding to a G-covariant normalized rank-1 POVM, i.e. $B = \{gv | g \in G\}$, then $T = \{w \cdot gv | g \in G\} = \{gw \cdot v | g \in G\}$ and the equality in (51) holds for all vectors from the orbit of w. Additionally, P is a G-invariant polynomial (see Sect. 4.1.4).

In consequence, if $-1/(d-1) \in T$ (respectively $-1/(d-1) \notin T$) and P attains its global minimum (maximum) in w, then w is also a global minimizer (maximizer) of F, since from (51) we get $F(u) \geq P(u) \geq P(w) = F(w)$ for every $u \in B(d)$. This method of finding global extrema was inspired by the one used in [**117**] for tetrahedral measurement (SIC-POVM in dimension two, $G = T_d$), where P is constant. Note, however, that a similar technique was used by Cohn, Kumar and Woo [**43, 44**] to solve the problem of potential energy minimization on the unit sphere. The whole idea can be traced back even further to [**166**] and [**2**]. At first look, it seems that we should be very fortunate to succeed using this method, because, first we need to guess where the global minimizer (maximizer) w is, then the corresponding set T needs to be of appropriate form, and finally not only P has to be minimized (maximized) by w, but also we need to be able to solve the minimization (maximization) problem for P. However, we shall see that all these constraints are, in many cases, not too restrictive.

Let us take a closer look at the family of functions satisfying (47). Obviously, if (47) holds for $f : [0,1] \to \mathbb{R}$, then it holds also for $\tilde{f} : [a,b] \ni t \mapsto f((t-a)/(b-a)) \in \mathbb{R}$, where $a < b \in \mathbb{R}$. Thus, we will be interested in functions defined on $[0,1]$. First of all, let us observe that the entropy function η belongs to this family. Another example of such a function is given by $\theta_\alpha(x) := (x - x^\alpha)/(\alpha - 1)$, where $0 < \alpha < 2$ and $\alpha \neq 1$. In consequence, our method can be applied both to the Havrda-Charvát-Tsallis α-entropy H_α and Rényi α-entropy R_α for $\alpha \in (0,2]$ (note that the function g_α defined in Example

3.2 is increasing in this interval), since both H_α and R_α can be modified in the same way as the Shannon entropy in Sect. 4.1.1 to be defined on the normalized Bloch set $B(d)$.

4.1.4. Group invariant polynomials. The material of this subsection is taken from [**58**, Ch. 3] and [**93**], see also [**67**]. Let G be a finite subgroup of the general linear group $GL_n(\mathbb{R})$. By $\mathbb{R}[x_1, \ldots, x_n]^G$ we denote the ring of G-invariant real polynomials in n variables. Its properties were studied by Hilbert and Noether at the beginning of twentieth century. In particular, they showed that $\mathbb{R}[x_1, \ldots, x_n]^G$ is finitely generated as an $\mathbb{R}$-algebra. Later, it was proven that it is possible to represent each G-invariant polynomial in the form $\sum_{j=1}^{m} P_j(\theta_1, \ldots, \theta_n)\,\eta_j$, where $\theta_1, \ldots, \theta_n$ are algebraically independent homogeneous G-invariant polynomials called *primary invariants*, forming so called *homogeneous system of parameters*, $\eta_1 = 1, \ldots, \eta_m$ are G-invariant homogeneous polynomials called *secondary invariants*, and P_j $(j = 1, \ldots, m)$ are elements from $\mathbb{R}[x_1, \ldots, x_n]$. Moreover, $\eta_1, \ldots, \eta_m$ can be chosen in such a way that they generate $\mathbb{R}[x_1, \ldots, x_n]^G$ as a free module over $\mathbb{R}[\theta_1, \ldots, \theta_n]$. Both sets of polynomials combined form so called *integrity basis*. Note that neither primary nor secondary invariants are uniquely determined. If $m = 1$, we call the basis *regular* and the group G *coregular*. The invariant polynomial functions on $\mathbb{R}^n$ separate the G-orbits. In consequence, the map $\mathbb{R}^n/G \ni Gx \to (\theta_1(x), \ldots, \theta_n(x), \eta_2(x), \ldots, \eta_m(x)) \in \mathbb{R}^{n+m-1}$ maps bijectively the orbit space onto an n-dimensional connected closed semialgebraic subset of $\mathbb{R}^{n+m-1}$. There is also a correspondence between the orbit stratification of $\mathbb{R}^n/G$ and the natural stratification of this semi-algebraic set into the primary strata, i.e. connected semialgebraic differentiable varieties. If $G \subset O(n)$ is a coregular group acting irreducibly on $\mathbb{R}^n$, we may assume that $\theta_1(x) = \sum_{i=1}^{n} x_i^2$ is a non-constant invariant polynomial of the lowest degree. Then the *orbit map* $\omega : S^{n-1}/G \ni Gx \to (\theta_2(x), \ldots, \theta_n(x)) \in \mathbb{R}^{n-1}$ is also one-to-one and its range is a semialgebraic $(n-1)$-dimensional set. In consequence, the minimizing of a G-invariant polynomial $P(x_1, \ldots, x_n)$ on S^{n-1} is equivalent to the minimizing of the respective polynomial $P_1(\theta_1, \ldots, \theta_n)$ on the range of ω. In the 1980s Abud and Sartori proposed a general procedure for finding the algebraic equations and inequalities defining this set and its strata, and thus also a general scheme for finding minima of P_1 on the range of the orbit map, see [**133, 134**].

Let us now take a closer look at the G-invariant polynomials of three real variables, which will be of our particular interest while considering HS-POVMs in dimension two. An element from $GL_n(\mathbb{R})$ is called a *pseudo-reflection*, if its fixed-points space has codimension one. The classical Chevalley-Shephard-Todd theorem says that every *pseudo-reflection* (i.e. generated by pseudo-reflections) *group* is coregular. As all the symmetry groups of polyhedra representing HS-POVMs in dimension two (D_{nh}, T_d, O_h, I_h) are pseudo-reflection groups, the interpolating polynomials can be expressed by their primary invariants listed below. Put $\rho := x^2 + y^2$, $\gamma_n := \Re\,(x+iy)^n$, $I_2 := x^2 + y^2 + z^2$, $I_3 := xyz$, $I_4 := x^4+y^4+z^4$, $I_6 := x^6+y^6+z^6$, $I_6' := (\tau^2x^2-y^2)(\tau^2y^2-z^2)(\tau^2z^2-x^2)$ and $I_{10} := (x+y+z)(x-y-z)(y-z-x)(z-y-x)(\tau^{-2}x^2-\tau^2y^2)(\tau^{-2}y^2-\tau^2z^2)(\tau^{-2}z^2-\tau^2x^2)$, where $\tau := (1+\sqrt{5})/2$ (the *golden ratio*). Note that the indices coincide with the degrees of invariant polynomials. Then (notation and results are taken from [**93**]) for the canonical representations of these groups, i.e. if coordinates x, y and z are so chosen that the origin is the fixed point for the group action and: the x and z axes are 2- and n-fold axes, respectively (D_{nh}); the 3-fold axes pass through vertices of a tetrahedron at $(1,1,1)$, $(1,-1,-1)$, $(-1,1,-1)$, $(-1,-1,1)$ (T_d); x, y and z axes are the 4-fold axes (O_h); the 5-fold axes pass through the vertices of an icosahedron at $(\pm\tau,\pm1,0)$, $0,\pm\tau,\pm1)$, $(\pm1,0,\pm\tau)$ (I_h), we get the primary invariants listed in Tab. 2:

group	primary invariants
D_{nh}	z^2,ρ,γ_n
T_d	I_2,I_3,I_4
O_h	I_2,I_4,I_6
I_h	I_2,I_6',I_{10}

TABLE 2. Primary invariants for four point groups.

In [**93**] the stratification of the range of the orbit map is analytically described in all these cases.

4.1.5. Majorization. Usually, the simplest way to find the entropy minimizers leads through the majorization technique. However, we shall see that this method fails in general and can be useful just in special cases.

Firstly, let us observe that for every pair of orthogonal states ρ and $\rho^\perp$ in $\mathcal{P}(\mathbb{C}^2)$ we have $(p_j(\rho,\Pi)+p_j(\rho^\perp,\Pi))/2 = 1/k$ for $j=1,\ldots,k$. Hence it follows that if the distribution of the measurement outcomes with the input state ρ majorizes that with the input state $\rho^\perp$, they must be equivalent, and so the entropies at these points are equal.

Moreover, if the POVM $\Pi = \{\Pi_j\}_{j=1}^k$ is tight informationally complete (i.e. the set of corresponding pure states is a complex projective 2-design), then for any $\rho \in \mathcal{S}(\mathcal{H})$ the probability distribution of measurement outcomes $(p_1(\rho,\Pi),\ldots, p_k(\rho,\Pi))$ fulfill an additional condition $p_1(\rho,\Pi)^2+\ldots+p_k(\rho,\Pi)^2 = 2d/(k(d+1))$. Thus, the set of all possible probability distributions is a $(2d-2)$-dimensional subset of the $(k-1)$-dimensional sphere of radius $2d/(k(d+1))$ intersected with the probability simplex Δ_k. That intersection is a $(k-2)$-dimensional sphere in the affine hyperplane containing Δ_k that is centered at the uniform distribution and, possibly, cutted to fit in the positive hyperoctant (compare Fig. 4 in [**8**]). Now, from the fact that the set of probability distributions majorized by a given $P \in \Delta_k$ is a convex hull of its orbit under permutations (see, e.g. [**24**, Ch. 2.1] or [**109**, Ch. 1.A]), it follows that the only probability distributions from the sphere indicated above that majorize (or are majorized by) any probability distribution from the same sphere need to be its permutations. Hence we deduce that if the distribution of measurement outcomes for one state majorizes that for another one, both distributions must be equivalent, and in particular the measurement entropies at these points are equal. These facts imply that the minimization problem cannot be solved in full generality via majorization.

On the other hand, the majorization technique can be used to reduce the minimization problem to a two-dimensional situation, if the Bloch representation of POVM in $\mathbb{C}^2$ is already two-dimensional.

Namely, we show that if B (defined in Sect. 4.1.1) is contained in a plane L, then H_B defined by (40) attains global minima on this plane. There is no loss of generality in assuming that $L = \mathbb{R}^2 \times \{0\}$. Put $w := (0,0,1)$. Since in this case $H_B(w) = H_B(-w) = \ln k$, it is enough to prove that $H_B(u) \geq H_B(\widetilde{u})$ for $u = (x,y,z) \neq w, -w$, where $\widetilde{u} := (x^2+y^2)^{-1}(x,y,0)$ is the normalized projection of u onto L. To this aim, it suffices to show that the probability vector $(p_1,\ldots,p_k)$ is majorized by the vector $(\tilde{p}_1,\ldots,\tilde{p}_k)$, where $p_j := (1+v_j\cdot u)/k$ and $\tilde{p}_j := (1+v_j\cdot\widetilde{u})/k$ for $j=1,\ldots,k$. Set $\alpha := x^2+y^2$. We have

$$p_j = (1+\alpha v_j\cdot\widetilde{u})/k = (1+\alpha(k\tilde{p}_j-1))/k = \alpha\tilde{p}_j + (1-\alpha)/k. \tag{52}$$

Let $\sigma : \{1,\ldots,k\} \to \{1,\ldots,k\}$ be a permutation such that $(\tilde{p}_{\sigma(1)},\ldots,\tilde{p}_{\sigma(k)})$ is decreasing. Then also $(p_{\sigma(1)},\ldots,p_{\sigma(k)})$ is decreasing and it is enough to prove that

$$\sum_{j=1}^{m}\tilde{p}_{\sigma(j)} \geq \sum_{j=1}^{m}p_{\sigma(j)} = \sum_{j=1}^{m}\left(\alpha\tilde{p}_{\sigma(j)} + (1-\alpha)/k\right), \tag{53}$$

for every $m = 1,\ldots,k$. But this is equivalent to $\sum_{j=1}^{m}\tilde{p}_{\sigma(j)} \geq m/k$, which is always true, since any probability vector majorizes $(1/k,\ldots,1/k)$.

4.2. Local extrema – dimension 2

For a finite group $G \subset \mathrm{O}(2)$ acting irreducibly on the sphere S^2 points lying on its rotation axes form the maximal strata, and so, it follows from Michel's theorem that they are critical for entropy functions. We can divide them into three categories depending on whether they are antipodal to the elements of the fiducial vector's orbit (type I), and, if not, whether their stabilizers act irreducibly on the tangent space (type II) or not (type III). In the first case, as well as, generically, in the second case, we can determine the character of critical point using the following proposition:

PROPOSITION 4.3. *Let $u \in S^2$ be a point lying on a rotation axis of the group $G \subset O(2)$ acting irreducibly on the sphere S^2 and let v denote the normalized Bloch vector of an arbitrary fiducial state for a rank-1 G-covariant POVM. Then:*

1) *If there exists $g \in G$ such that $u = -gv$, then u is a local minimizer (resp. maximizer) for H_v (resp. $\widetilde{H}_v$);*
2) *If $u \neq -gv$ for every $g \in G$ and the linear isotropy group $\{T_u g : g \in G_u\}$ acts irreducibly on $T_u S^2$ (or, equivalently, G_u contains a cyclic subgroup of order greater than 2), then:*
   (a) if
$$\frac{2}{|G/G_u|} \sum_{[h] \in G/G_u} (hu \cdot v) \ln(1 + hu \cdot v) > 1, \tag{54}$$
   then u is a local minimizer (resp. maximizer) for H_v (resp. $\widetilde{H}_v$),
   (b) if
$$\frac{2}{|G/G_u|} \sum_{[h] \in G/G_u} (hu \cdot v) \ln(1 + hu \cdot v) < 1, \tag{55}$$
   then u is a local maximizer (resp. minimizer) for H_v (resp. $\widetilde{H}_v$).

PROOF. Fix any geodesic (i.e. a great circle) passing by u. Let q be one of two vectors lying on the intersection of the plane orthogonal to u passing through 0 and the geodesic. As 0 is the only G-invariant vector in $\mathbb{R}^3$ and, at the same time, the only G_u-invariant element orthogonal to u, we have $(1/|G_u|) \sum_{g \in G} gu = \sum_{[h] \in G/G_u} hu = 0 = \sum_{g \in G_u} gq$. Consider a natural parametrisation of the great circle $\gamma : (-\pi, \pi) \to \mathbb{S}^2$ (throwing away $-u$) given by $\gamma(\delta) := (\sin \delta) q + (\cos \delta) u$ for $\delta \in (-\pi, \pi)$, where δ is the measure of the angle between vectors u and $\gamma(\delta)$. Put $w := \gamma(\delta)$. Then it follows from (42), (43) and the equality $\sum_{g \in G} gw = 0$ that

$$\begin{aligned}
(H_v \circ \gamma)(\delta) &= H_v(w) \\
&= \ln \frac{|G|}{2} + \frac{2}{|G|} \sum_{g \in G} \eta((1 + gw \cdot v)/2) \\
&= \ln |G| + \frac{1}{|G|} \sum_{g \in G} \eta(1 + gw \cdot v) \\
&= \ln |G| + \frac{1}{|G|} \sum_{[h] \in G/G_u} \sum_{g \in Gu} \eta(1 + hgw \cdot v) \\
&= \ln |G| + \frac{1}{|G|} \sum_{[h] \in G/G_u} \sum_{g \in Gu} \eta(1 + (\sin \delta) hgq \cdot v + (\cos \delta) hu \cdot v) \\
&= \ln |G| + \frac{1}{|G/G_u|} \sum_{[h] \in G/G_u} f_h(\delta),
\end{aligned}$$

where

$$f_h(\delta) := \frac{1}{|G_u|} \sum_{g \in G_u} \eta(1 + (\sin\delta) hgq \cdot v + (\cos\delta) hu \cdot v).$$

Let $h \in G$ be such that $hu \neq -v$. Then, for δ small enough, we get

$$\begin{aligned} f_h'(\delta) = \frac{1}{|G_u|} \sum_{g \in G_u} \eta'(1 + (\sin\delta) hgq \cdot v + (\cos\delta) hu \cdot v) \times \\ \times ((\cos\delta) hgq \cdot v - (\sin\delta) hu \cdot v). \end{aligned}$$

In particular $f_h'(0) = 0$. Moreover,

$$\begin{aligned} f_h''(\delta) = & \frac{1}{|G_u|} \sum_{g \in G_u} \eta''(1 + (\sin\delta) hgq \cdot v + (\cos\delta) hu \cdot v) \times \\ & \times ((\cos\delta) hgq \cdot v - (\sin\delta) hu \cdot v)^2 + \\ & + \eta'(1 + (\sin\delta) hgq \cdot v + (\cos\delta) hu \cdot v)(-(\sin\delta) hgq \cdot v - (\cos\delta) hu \cdot v)). \end{aligned}$$

1) Let $\widetilde{h}u = -v$ for some $\widetilde{h} \in G$. Then $\widetilde{h}gq \cdot v = 0$ and so $f_{\widetilde{h}}(\delta)$ reduces to

$$f_{\widetilde{h}}(\delta) = 1/|G_u| \sum_{g \in G_u} \eta(1 - \cos\delta).$$

In consequence, for $\delta \neq 0$

$$f_{\widetilde{h}}'(\delta) = -(\ln(1 - \cos\delta) + 1) \sin\delta,$$

and so

$$f_{\widetilde{h}}''(\delta) = -1 - (\cos\delta)(\ln(1 - \cos\delta) + 2).$$

Since $f_{\widetilde{h}}'(\delta) \to 0$ as $\delta \to 0$, so $f_{\widetilde{h}}'(0) = 0$. Moreover, $f_{\widetilde{h}}''(\delta) \to \infty$ as $\delta \to 0$. Let us observe that there exists $1 > c > 0$, such that the inequality $hu \cdot v \geq -1 + c$ holds for any $[h] \in G/G_u$, $[h] \neq [\widetilde{h}]$. Now we can estimate $|f_h''(\delta)|$ as follows:

$$\begin{aligned} |f_h''(\delta)| \leq & \frac{1}{|G_u|} \sum_{g \in G_u} \left| \frac{((\cos\delta) hgq \cdot v - (\sin\delta) hu \cdot v)^2}{1 + hgw \cdot v} \right| \\ & + \frac{1}{|G_u|} \sum_{g \in G_u} |(\ln(1 + hgw \cdot v) + 1)(hgw \cdot v)| \\ \leq & \frac{1}{|G_u|} \sum_{g \in G_u} \left(\frac{1}{|1 + hgw \cdot v|} + (|\ln(1 + hgw \cdot v)| + 1) \right) \\ \leq & f\left(1 - |\sin\delta| + (c-1)\cos\delta\right), \end{aligned}$$

for $|\delta| < c$, where $f(x) := \frac{1}{|x|} + |\ln x| + 1$ for $x > 0$. The last inequality follows from the fact that f is decreasing in $(0,1)$, $1 + hgw \cdot v \geq 1 - |\sin\delta| + (c-1)\cos\delta$ and $1 - |\sin\delta| + (c-1)\cos\delta \geq 0$ for $|\delta| < c$.

Thus

$$
\begin{aligned}
(H_v \circ \gamma)''(\delta) &= \frac{1}{|G/G_u|}\left(f''_{\widetilde{h}}(\delta) + \sum_{[h]\in G/G_u, [h]\neq[\widetilde{h}]} f''_h(\delta) \right) \\
&\geq g\,(\delta) \overset{\delta\to 0}{\longrightarrow} +\infty,
\end{aligned}
$$

where

$$
g\,(\delta) := -\frac{1+(\cos\delta)(\ln(1-\cos\delta)+2)+(|G/G_u|-1)f(1-\sin\delta+(c-1)\cos\delta)}{|G/G_u|}
$$

for $\delta > 0$. In particular, $(H_v \circ \gamma)'(0) = 0$ and there is $\varepsilon > 0$ such that $(H_v \circ \gamma)''(\delta) > 0$ for $|\delta| < \varepsilon$. Hence, one can find a neighbourhood $\mathcal{V} \subset S^2$ of u such that for any geodesic passing by u, H_v is strictly convex on its part contained in $\mathcal{V}$ and has minimum at u. Consequently, $H_v(u) > H_v(w)$ for every $w \in \mathcal{V}$, $w \neq u$, which completes the proof of 1).

2) Assume that $u \neq -gv$ for every $g \in G$ and the linear isotropy group $\{T_u g : g \in G_u\}$ acts irreducibly on $T_u S^2$. Then for every $h \in G$ we have

$$
\begin{aligned}
f''_h(0) &= \frac{1}{|G_u|}\sum_{g\in G_u} (\eta''(1+hu\cdot v)(hgq\cdot v)^2 + \eta'(1+hu\cdot v)(-hu\cdot v)) \\
&= \eta'(1+hu\cdot v)(-hu\cdot v) + \eta''(1+hu\cdot v)\frac{1}{|G_u|}\sum_{g\in G_u}(hgq\cdot v)^2 \\
&= (hu\cdot v)(\ln(1+hu\cdot v)+1) - \frac{1}{1+hu\cdot v}\frac{1}{2}(1-(hu\cdot v)^2) \\
&= (hu\cdot v)(\ln(1+hu\cdot v)+3/2) - 1/2,
\end{aligned}
$$

where the last but one identity follows from the fact that $\{hgq : g \in G_u\}$ is a normalized tight frame in S^2 contained in the plane orthogonal to hu for each $h \in G_u$. Thus we obtain

$$
(H_v \circ \gamma)''(0) = \frac{1}{|G/G_u|}\sum_{[h]\in G/G_u}(hu\cdot v)\ln(1+hu\cdot v) - 1/2
$$

and 2) follows from the Modern Purkiss Principle. □

If Π is a HS-POVM, we can assume that G is one of the following groups: D_{nh}, T_d, O_h or I_h, and the Bloch vector of the fiducial vector v lies in the maximal strata, consisting of points where the rotation axes of the group intersect the Bloch sphere. For D_{nh} group we have one n-fold and n 2-fold rotation axes ($2n+2$ points: a digon and two regular n-gons); for T_d group: three 2-fold, four 3-fold rotation axes (14 points: an octahedron and two dual tetrahedra); for O_h group: six 2-fold, four 3-fold, three 4-fold rotation axes (26 points: a cuboctahedron, a cube and an octahedron); for I_h group: fifteen 2-fold, ten 3-fold, six 5-fold rotation axes (62 points: an icosidodecahedron, a dodecahedron and an icosahedron). The character of these singularities is described by the following proposition.

PROPOSITION 4.4. *In the situation above, singular points of type I are minima (resp. maxima), of type II maxima (resp. minima), and of type III saddle points for H_B (resp. $\widetilde{H}_B$).*

The proof of this fact is quite elementary. From Proposition 4.3.1) we deduce the character of singular points of type I. For type II it is enough to use Proposition 4.3.2). For type III one have to indicate two great circles such that the second derivatives along these curves have different sign. As we will not use this fact in the sequel, we omit the details.

Hence the points of type I are the natural candidates for minimizing H_B (resp. maximizing $\widetilde{H}_B$), and indeed, we will show in the next section that they are global minimizers (resp. maximizers). However, if a POVM is merely symmetric, the global extrema of entropy functions may also occur in other (non inert) points. An example of this phenomenon can be found in [**70**], see also [**29, 173**]. Let us consider a symmetric (but non-highly symmetric) POVM generated by the set of four Bloch vectors forming a rectangle $B = \{v_1, -v_1, v_2, -v_2\}$, where $v_1, v_2 \in S^2$, $v_1 \notin \{-v_2, v_2\}$, and $v_1 \cdot v_2 \neq 0$, with $\mathrm{Sym}\,(B) \simeq D_{2h}$ having three mutually perpendicular 2-fold rotation axis. In this way we get six vectors in S^2 that are necessarily critical for H_B and $\widetilde{H}_B$: two perpendicular both to v_1 and to v_2, and four lying in the plane generated by v_1 and v_2, proportional to $\pm v_1 \pm v_2$. The former are local maxima of H_B, and the latter either local minima or saddle points, depending on the value of the parameter $\alpha := \arccos\,(v_1 \cdot v_2) \in (0, \pi)$, $\alpha \neq \pi/2$. Let $\overline{\alpha} \approx 1.17056$ be a unique solution of the equation $(\cos(\overline{\alpha}/2)) \ln(\tan^2(\overline{\alpha}/4)) = -2$ in the interval $(0, \pi/2)$. In [**70**] the authors showed that for $\alpha \in (0, \overline{\alpha}]$ the function H_B (resp. $\widetilde{H}_B$) attains the global minimum (resp. maximum) at the points $\pm\,(v_1 + v_2)\,/\,(2\,|\cos\,(\alpha/2)|)$, whereas $\pm\,(v_1 - v_2)\,/\,(2\,|\sin\,(\alpha/2)|)$ are saddle points, and for $\alpha \in [\pi - \overline{\alpha}, \pi)$ the situation is reversed. However, for $\alpha \in (\overline{\alpha}, \pi - \overline{\alpha})$ all these inert states become saddles, and two pairs of new global minimizers emerge, lying symmetrically with respect to the old ones. The appearance of this pitchfork bifurcation phenomenon shows also that, in general, one cannot expect an analytic solution of the minimization problem in a merely symmetric case. This is why we restrict our attention to highly symmetric POVMs.

Note also that for highly symmetric POVMs we can use, instead of full symmetry group $\mathrm{Sym}\,(B)$, any subgroup acting transitively on B, e.g. C_n for the regular n-gon, T for the tetrahedron, O for the cuboctahedron, cube and octahedron, and I for the icosidodecahedron, dodecahedron and icosahedron. They have the same rotation axes as the full symmetry groups.

4.3. Global minima

4.3.1. The Hermite interpolation method for HS-POVMs in dimension 2. We apply the general method described in Sect. 4.1.3 in our situation.

We will interpolate the function $h : [-1,1] \to \mathbb{R}^+$ defined by (42) choosing the interpolation points from the set $T := \{-gv \cdot v | g \in G\} \subset [-1,1]$, where v is the Bloch vector representation of the fiducial vector and $-v$ is supposed to be the Bloch vector of a global minimizer (by Proposition 4.3 we already know that it is a local minimizer). We must distinguish two situations: either the inversion $-I \in G$ (equivalently $-v \in B$) or not. The former is the case for $G = D_{nh}$ (for even n), O_h, I_h, and then $1 \in T$, the latter for $G = D_{nh}$ (for odd n), T_d, and then $1 \notin T$. After reordering the elements of T we obtain an increasing sequence $\{t_i\}_{i=1}^m$, where $m := |T|$. In particular, $t_1 = -1$. Taking in (45) $k_i = 1$ for $t_i \in \{-1,1\}$ and $k_i = 2$ otherwise, we obtain the Hermite interpolating polynomial p_v that interpolates h from below and agrees with h for $t \in T$, see the illustration of this for the octahedral POVM in Fig. 3. The degree of p_v is bounded by $D(v) := 2m - 2$, if $1 \in T$, and $D(v) := 2m - 1$, otherwise.

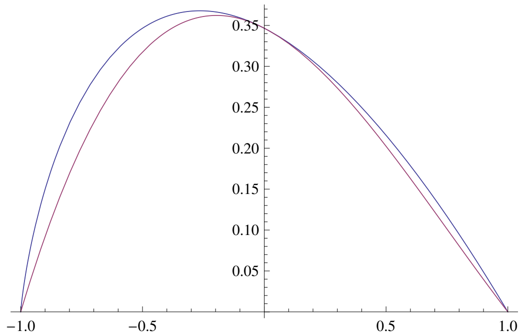

FIGURE 3. The cubic polynomial function p_v (*purple*) interpolating h (*violet*) from below for the octahedral measurement, with $t_1 = -1$, $t_2 = 0$ and $t_3 = 1$.

Let us consider the G-invariant polynomial $P_v : \mathbb{R}^3 \to \mathbb{R}$ given by replacing h in (43) by p_v, i.e.

$$P_v(u) := \ln \frac{|G|}{2} + \frac{2}{|G|} \sum_{g \in G} p_v(gv \cdot u) \tag{56}$$

for $u \in \mathbb{R}^3$. It interpolates H_v from below while restricted to the unit sphere (Bloch sphere). Moreover, $H_v(-gv) = P_v(-gv) = P_v(-v)$ for $g \in G$. In consequence, now it is enough to show that $-v$ is a global minimizer of P (and hence all the elements of its orbit $\{-gv : g \in G\}$ are).

Of course, the lower the degree of the interpolating polynomial p_v is, the easier it is to find the minima of P_v, as $\deg P_v \leq \deg p_v$. The last quantity in turn depends on the cardinality of $T := \{-gv \cdot v | g \in G\}$, that can be calculated by analyzing double cosets of isotropy subgroups of any subgroup $K \subset G \cap SO(3)$ acting transitively on B, because $T = \{-gv \cdot v | g \in K\}$ and for $h, g \in K$, if h is in a double coset $K_v g K_v$ or $K_v g^{-1} K_v$, then $hv \cdot v = gv \cdot v$. Hence $|T| \leq n(v) := n_s(v) + \frac{1}{2} n_a(v)$, where $n_s(v)$ is the number of self-inverse double cosets of

K_v, i.e. the cosets fulfilling $K_v g K_v = K_v g^{-1} K_v$, and $n_a(v)$ is the number of non self-inverse ones. Thus

$$\deg p_v \leq \begin{cases} 2n(v) - 3, & \text{if } -v \in Kv \\ 2n(v) - 2, & \text{if } -v \notin Kv \end{cases} . \tag{57}$$

Moreover, for $g \in K$, using the well-known formula for the cardinality of a double coset, see, e.g. [**28**, Prop. 5.1.3], we have $|K_v g K_v| = |K_v| \, |K_v / (K_v \cap K_{gv})| = |K_v|$, if $gv = v$ or $gv = -v$, and $|K_v|^2$, otherwise. Hence, if $-v \in Kv$, then $|Kv| \, |K_v| = |K| = 2 \, |K_v| + (n_s(v) - 2) \, |K_v|^2 + n_a(v) \, |K_v|^2$, and so $n_s(v) + n_a(v) = (|Kv| - 2) \, / \, |K_v| + 2$. Analogously, if $-v \notin Kv$, then we have $n_s(v) + n_a(v) = (|Kv| - 1) \, / \, |K_v| + 1$. Using these facts and (57) we get finally

$$\deg p_v \leq \begin{cases} \frac{|Kv|-2}{|K_v|} + n_s(v) - 1, & \text{if } -v \in Kv \\ \frac{|Kv|-1}{|K_v|} + n_s(v) - 1, & \text{if } -v \notin Kv \end{cases} . \tag{58}$$

Applying (58) to HS-POVMs in dimension two we get the upper bounds for the degree of interpolating polynomials gathered in Tab. 3.

Kv	$\|Kv\|$	K	K_v	$n_a(v)$	$n_s(v)$	$n(v)$	$\deg p_v \leq$
regular n-gon (n-even)	n	C_n	C_1	$n-2$	2	$n/2+1$	$n-1$
regular n-gon (n-odd)	n	C_n	C_1	$n-1$	1	$n/2+1/2$	$n-1$
tetrahedron	4	T	C_3	0	2	2	2
octahedron	6	O	C_4	0	3	3	3
cube	8	O	C_3	0	4	4	5
cuboctahedron	12	O	C_2	4	3	5	7
icosahedron	12	I	C_5	0	4	4	5
dodecahedron	20	I	C_3	4	4	6	9
icosidodecahedron	30	I	C_2	14	2	9	15

TABLE 3. HS-POVMs in dimension two: upper bounds for the number of interpolating points ($n(v)$) and the degree of interpolating polynomial.

To find global minimizers of P_v we can express the polynomial in terms of primary and secondary invariants for the corresponding ring of G-invariant polynomials. In fact, as we will see in the next section, only the former will be used.

4.3.2. The main theorem.

THEOREM 4.5. *For HS-POVMs in dimension two the points lying on the orbit of the point antipodal to the Bloch vector of the fiducial vector (that is the Bloch vector of the state orthogonal to the fiducial vector) are the only global minimizers (resp. maximizers) for the entropy of measurement (resp. the relative entropy of measurement).*

Proof. We will give a proof of the theorem in two steps. Firstly, we show that the antipodal points to the Bloch vectors of POVM elements, i.e. the points $\{-gv : g \in G\}$ are the global minima of the G-invariant polynomial P_v constructed in Sect. 4.3.1. (In particular, this is true if P_v is constant.) Then we prove the uniqueness of designated global minimizers of the entropy of measurement.

We shall use the a priori estimates for $\deg P_v$ that can be read from Tab. 3 and the primary invariants of G listed in Tab. 2. We may exclude the trivial case when the HS-POVM in question is PVM represented by two antipodal points on the Bloch sphere (digon), as in this situation the minimal value of H equal 0 is achieved at these points and the assertion follows. The proof is divided into four cases according to the symmetry group of the HS-POVM.

Case I (prismatic symmetry)

Regular n-gon. In Sect. 4.2 we showed that in this case it is enough to look for the global minimizers on the circle $S^1 := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ containing the n-gon. Its symmetry group acts on the plane $z = 0$ as the dihedral group D_n, and so the interpolating polynomial P_v restricted to the circle S^1 can be expressed in terms of its primary invariants, i.e. $\rho = x^2 + y^2$ and $\gamma_n = \Re(x + iy)^n$. Since $\deg P_v < n$, it follows that $P_v|_S$ has to be a linear combination of ρ^m, $0 \leq 2m < n$, and hence constant.

Case II (tetrahedral symmetry)

Tetrahedron. This case is immediate, as $\deg P_v \leq \deg p_v \leq 2$, and so P_v has to be constant on the sphere S^2.

Case III (octahedral symmetry)

For O_h we have inert states at the O_h-orbits of the points: $x_1 := (0, 0, 1)$ (vertices of an octahedron), $x_2 := \frac{1}{\sqrt{2}}(0, 1, 1)$ (vertices of a cuboctahedron), and $x_3 := \frac{1}{\sqrt{3}}(1, 1, 1)$ (vertices of a cube). Using the Lagrange multipliers it is easy to check that these points are the only critical points for I_4 and I_6 restricted to the sphere S^2. By comparing the values of I_4 and I_6 (which are $I_4(x_1) = 1$, $I_4(x_2) = 1/2$, $I_4(x_3) = 1/3$, $I_6(x_1) = 1$, $I_6(x_2) = 1/4$, $I_6(x_3) = 1/9$), we find that the points lying on the orbit of x_3 are global minimizers both for I_4 and I_6.

Octahedron. This case is straightforward, as for $v = x_1$ we have $\deg P_v \leq \deg p_v \leq 3$, and so P_v has to be constant on the sphere S^2.

Cube. In this case we have $v = x_3$ and $\deg P_v \leq \deg p_v \leq 5$. In consequence, P_v must be a linear combination of 1, I_2, I_4, and I_2^2. After the restriction to the sphere, $P_v|_{S^2}$ can be expressed as $A + BI_4$, for some $A, B \in \mathbb{R}$. Thus, all we need to know now is the sign of B. Calculating the values of P_v in two points from different orbits (e.g. x_1 and x_3) and solving the system of two linear equations we get $B = (3/8)\ln(27/16) > 0$. Thus the global minimizers for P_v are the same as for I_4, i.e. they lie on the orbit of v or, equivalently, $-v$, as required.

Cuboctahedron. For the cuboctahedral measurement we have $v = x_2$ and $\deg P_v \leq \deg p_v \leq 7$. Consequently, $\deg P_v \leq 6$ and P_v is a linear combination of 1, I_2, I_4, I_2^2, I_6, $I_4 I_2$, and I_2^3. Hence, after the restriction to the sphere S^2, we get $P_v|_{S^2} = A + BI_4 + CI_6$, for some $A, B, C \in \mathbb{R}$. Put $\beta := -B/(3C)$. Clearly, all inert states are critical for $P_v|_{S^2}$ with $P_v(x_1) = A + C(1 - 3\beta)$, $P_v(x_2) = A + C(1 - 6\beta)/4$, $P_v(x_3) = A + C(1 - 9\beta)/9$. One can show easily that they are only critical points unless $1/4 < \beta < 1/2$. In this case there are another critical points, namely the orbit of the point $x_4 := \left(\sqrt{4\beta - 1}, \sqrt{1 - 2\beta}, \sqrt{1 - 2\beta}\right)$ with $P_v(x_4) = C\left(1 - 9\beta + 24\beta^2 - 24\beta^3\right)$. To find B and C, we need to calculate the values of P_v in three points from different orbits (e.g. x_1, x_2 and x_3) and to solve the system of three linear equations. In this way we get $B = \frac{520}{9}\ln 2 - 37\ln 3 < 0$, $C = -\frac{364}{9}\ln 2 + 26\ln 3 > 0$ and $\beta \approx 0.3775$. Comparison of the values that P_v achieves at points x_1, x_2, x_3 and x_4 leads to the conclusion that the global minima are achieved for the vertices of cuboctahedron that form the orbit of v and thus also of $-v$.

Case IV (icosahedral symmetry)

The inert states for I_h, that is the I_h-orbits of points: $x_1 = (0, 0, 1)$ (vertices of an icosidodecahedron), $x_5 := \frac{1}{\sqrt{\tau+2}}(0, \tau, 1)$ (vertices of an icosahedron), and $x_6 := \frac{1}{\sqrt{3}}(0, \frac{1}{\tau}, \tau)$ (vertices of a dodecahedron) are the only critical points for I_6'. They are, correspondingly, saddle, minimum, and maximum points with values: 0, $-(2 + \sqrt{5})/5$, and $(2 + \sqrt{5})/27$, respectively. For I_{10}, the I_h-orbit of x_6 also coincides with the set of the global maxima, and we have local maxima at the I_h-orbit of x_5 and saddle points at the orbit of x_1, but there are also non-inert critical points, namely sixty minima at the vertices of a non-Archimedean vertex truncated icosahedron (Fig. 14 in [**170**]), and sixty saddles at the vertices of an edge truncated Archimedean vertex truncated icosahedron (Fig. 5 in [**169**]), see [**93**, p. 26].

Icosahedron. This case is immediate, as $v = x_5$ and $\deg P_v \leq \deg p_v \leq 5$. Hence P_v restricted to S^2 is constant.

Dodecahedron. In this case $v = x_6$ and $\deg P_v \leq \deg p_v \leq 9$. Therefore P_v must be a linear combination of 1, I_2, I_2^2, I_2^3, I_6', I_2^4 and $I_6' I_2$. After restriction to S^2 we obtain $P_v|_{S^2} = A + BI_6'$, for some $A, B \in \mathbb{R}$. We can calculate B using the same method as in the cubical case. As it turns out to be negative ($B \approx -0.06509$), the global minimizers coincide with the global maximizers for I_6', i.e. they are the vertices of the dodecahedron.

Icosidodecahedron. The icosidodecahedral case ($v = x_1$) is the most complicated one. Since $\deg P_v \leq \deg p_v \leq 15$, and P_v must be a linear combination of polynomials 1, I_2, I_2^2, I_2^3, I_6', I_2^4, $I_6' I_2$, I_2^5, $I_6' I_2^2$, I_{10}, I_2^6, $I_6' I_2^3$, $(I_6')^2$, $I_{10} I_2$, I_2^7, $I_6' I_2^4$, $(I_6')^2 I_2$, and $I_{10} I_2^2$. Restriction to S^2 gives us: $P_v|_{S^2} = A + BI_6' + CI_{10} + D(I_6')^2$, for some $A, B, C, D \in \mathbb{R}$. Both of the polynomials I_6' and I_{10} take the value 0 at

x_1, which is obviously a critical point for $P_v|_{S^2}$. As we have conjectured that the vertices of the icosidodecahedron are the global minimizers of $P_v|_{S^2}$, it is enough to prove that $\tilde{P} := P_v|_{S^2} - A$ is nonnegative. We keep proceeding like in the previous cases to obtain formulae for B, C, and D:

$$\begin{aligned} B =& -(1/50)(-2+\sqrt{5})(7122\sqrt{5}\,\mathrm{arcoth}(\sqrt{5}) + 3(-3728+2773\sqrt{5})\ln 2 \\ &+ 39575\ln 3 - 4700\ln 5 - 8319\sqrt{5}\ln(7+3\sqrt{5})), \\ C =&(1/180)(-108414\,\mathrm{arcoth}(3/\sqrt{5}) + 47970\,\mathrm{arcoth}(\sqrt{5}) + \sqrt{5}(-16352\ln 2 \\ &+ 51120\ln 3 - 5265\ln 5)), \\ D =&(29/900)(9-4\sqrt{5})(53766\sqrt{5}\,\mathrm{arcoth}(3/\sqrt{5}) - 23418\sqrt{5}\,\mathrm{arcoth}(\sqrt{5}) \\ &+ 34816\ln 2 - 126450\ln 3 + 15075\ln 5). \end{aligned}$$

The range Ω of the orbit map $\omega : S^2/I_h \ni I_h w \to (I_6'(w), I_{10}(w)) \in \mathbb{R}^2$ is the curvilinear triangle (see Fig. 4) defined by the following inequalities imposed on the coordinates $(\theta_1, \theta_2) \in \mathbb{R}^2$:

$$-\frac{2\tau+1}{5} \leq \theta_1 \leq \frac{2\tau+1}{27}, \quad (7-4\tau)\theta_1 \leq \theta_2, \tag{59}$$

$$\begin{aligned} 0 \leq J_{15}^2 :=& 4\theta_1^2 - 8(3+4\tau)\theta_1\theta_2 - 91(3-2\tau)\theta_1^3 + 4(5+8\tau)\theta_2^2 + \\ &+ 159(1-2\tau)\theta_1^2\theta_2 + 688(13-8\tau)\theta_1^4 + 325(1+2\tau)\theta_1\theta_2^2 + \\ &- 720(7-4\tau)\theta_1^3\theta_2 - 1728(55-34\tau)\theta_1^5 - 25(11+18\tau)\theta_2^3, \end{aligned}$$

where J_{15} is the only secondary invariant for the icosahedral group I [**93**, Tab. IIIb].

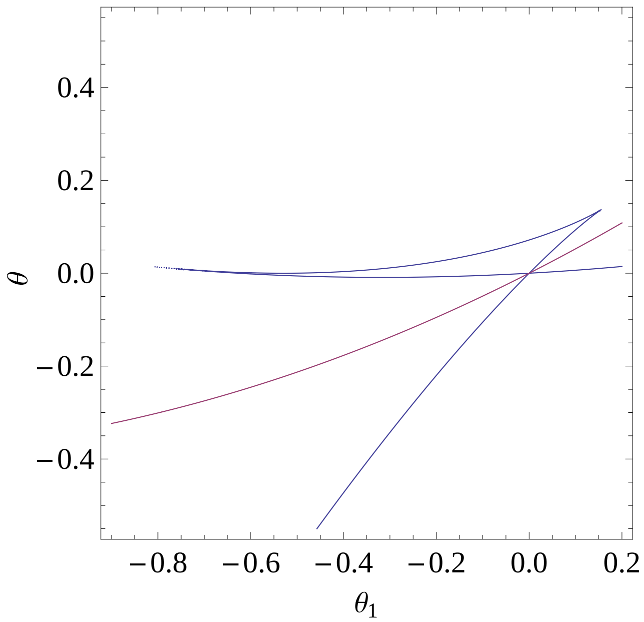

FIGURE 4. The zero level set for P_1 (*purple*) and for J_{15}^2 (*violet*).

Define $P_1(\theta_1,\theta_2) := B\theta_1 + C\theta_2 + D\theta_1^2$ for $(\theta_1,\theta_2) \in \Omega$. Then $\tilde{P}(w) = P_1(\omega((I_h)w))$ for $w \in S^2$. The level sets of P_1 are parabolas and the zero level parabola given by $\theta_2 = -(B/C)\theta_1 - (D/C)\theta_1^2$ (the purple curve in Fig. 4) divides the plane into two regions: $\{P_1 \geq 0\}$ and $\{P_1 < 0\}$. Now, it is enough to show that the zero level set of P_1 meets with the zero level set of J_{15}^2 (the violet curve in Fig. 4), which defines the boundary of Ω only at $(\theta_1,\theta_2) = (0,0)$, since in this case P_1 has the same sign over the whole Ω, and, in consequence, $\tilde{P}$ is positive on the whole unit sphere. This approach reduces the complexity of the problem by lowering the degree of a polynomial equation to be solved. In fact, now it is enough to show that the polynomial $Q(\theta_1) := J_{15}^2\left(\theta_1, -(B/C)\theta_1 - (D/C)\theta_1^2\right)/\theta_1^2$ of degree 4 has no real roots. This can be done in a standard way by using Sturm's theorem, the method which we recall briefly below.

The *Sturm chain* for polynomial q is a sequence $q_0, q_1, \ldots, q_m$, where $q_0 = q$, $q_1 = q'$, $q_i = -\mathrm{rem}(q_{i-2}, q_{i-1})$ for $i = 2, \ldots, m$, and $m \leq \deg q$ is the minimal number i such that $\mathrm{rem}(q_{i-1}, q_i) = 0$ (by $\mathrm{rem}(r,s)$ we denote the reminder of division of r by s). Sturm's theorem states that the number of roots of q in (a,b) for $-\infty \leq a < b \leq +\infty$ equals to the difference between the numbers of sign changes in the Sturm chain for q evaluated in b and a (for more details see, e.g. [**20**, Sect. 2.2]). Thus, to finish the proof for icosidodecahedron, we calculate Sturm's chain for Q, evaluate it at $\pm\infty$ and show that numbers of sign changes do not differ.[2]

We end the proof with showing that there are no other (global) minimizers of the entropy.

It follows from (51) that if $w \in S^2$ is a global minimizer for H_v, then it is also a global minimizer for P_v, since $P_v(-v) \leq P_v(w) \leq H_v(w) = H_v(-v) = P_v(-v)$. The same argument gives us $h(w \cdot u) = p(w \cdot u)$ for every $u \in Gv$, and so $\{w \cdot u : u \in Gv\} \subset T = \{-v \cdot u : u \in Gv\}$.

Put $a_u := w \cdot u$ for $u \in Gv$ and $k := |Gv|$. Now it is enough to show that $-1 \in T_w := \{a_u : u \in Gv\}$, since then $w \in G(-v)$. We know that $\sum_{u \in Gv} a_u = 0$. For informationally-complete HS-POVMs we have additionally $\sum_{u \in Gv} a_u^2 = k/3$ (as Gv is 2-design), and, for icosahedral group, $\sum_{u \in Gv} a_u^4 = k/5$ (as Gv is 4-design). Moreover, $1 \in T_w$ implies $-1 \in T_w$ for octahedral and icosahedral group. Using all these facts and the form of the interpolating set for respective informationally complete HS-POVMs (see Tab. 4) we see that in all seven cases the assumption $-1 \notin T_w$ leads to the immediate contradiction. On the other hand, for a regular polygon w must lie on the circle containing this polygon (see Sect. 4.1.5). Then $w \cdot (-v) \in T$, implies $w \in G(-v)$, as desired.

$\square$

[2] To determine the signs of complicated expressions the *Mathematica* command `Sign` has been used.

Gv	$\lvert Gv\rvert$	T
regular n-gon (n even)	n	$\left\{\cos\left(\frac{2\pi j}{n}\right) : j = 1, \ldots, n\right\}$
regular n-gon (n odd)	n	$\left\{-\cos\left(\frac{2\pi j}{n}\right) : j = 1, \ldots, n\right\}$
tetrahedron	4	$\left\{-1, \frac{1}{3}\right\}$
octahedron	6	$\{-1, 0, 1\}$
cube	8	$\left\{-1, -\frac{1}{3}, \frac{1}{3}, 1\right\}$
cuboctahedron	12	$\left\{-1, -\frac{1}{2}, 0, \frac{1}{2}, 1\right\}$
icosahedron	12	$\left\{-1, -\frac{1}{\sqrt{5}}, \frac{1}{\sqrt{5}}, 1\right\}$
dodecahedron	20	$\left\{-1, -\frac{\sqrt{5}}{3}, -\frac{1}{3}, \frac{1}{3}, \frac{\sqrt{5}}{3}, 1\right\}$
icosidodecahedron	30	$\left\{-1, -\frac{\tau}{2}, -\frac{1}{2}, -\frac{1}{2\tau}, 0, \frac{1}{2\tau}, \frac{1}{2}, \frac{\tau}{2}, 1\right\}$

Table 4. The interpolating sets for HS-POVMs in dimension two.

Remark 4.1. Let us observe that without any additional calculations we get that the theorem holds true for POVMs represented by regular polygons, tetrahedron, octahedron and icosahedron if the Shannon entropy is replaced by Havrda-Charvát-Tsallis α-entropy or Rényi α-entropy for $\alpha \in (0, 2]$. It follows from the fact that the degree of the polynomial P_v interpolating generalised entropy or its increasing function from below (see Sect. 4.1.3) does not depend on the entropy function. As in all these cases it is at most 2, thus P is constant.

4.4. Global minima – SIC-POVMs in dimension 3

The first result we present here is strictly connected with the geometry of SIC-POVMs in dimension three and does not involve any algebraic structure. Though, the assumption of this theorem concerning linear dependency among the vectors defining a SIC-POVM is not at any rate obvious. However, it follows from [**50**, Thm 1] that this assumption is fulfilled if a SIC-POVM is covariant with respect to the Weyl-Heisenberg group and its fiducial vector is an eigenvector of certain canonical order 3 unitary conjugated to $U_{\mathcal{Z}}$, which is not a huge restriction since all known SIC-POVMs in dimension three are of this form.

Theorem 4.6. *Let* $\Pi = \{(1/3)|\phi_j\rangle\langle\phi_j|\}_{j=1}^{9}$ *be a SIC-POVM in dimension three and let us assume that some three out of nine vectors* $|\phi_j\rangle$ *are linearly dependent. Then the state* $|\psi\rangle\langle\psi|$*, where* $|\psi\rangle$ *is orthogonal to the two-dimensional subspace spanned by these vectors, minimizes (resp. maximizes) the entropy of* Π *(resp. the relative entropy of* Π*). Moreover, all global minimizers (resp. maximizers) are of this form.*

PROOF. Let us assume that $|\phi_1\rangle, |\phi_2\rangle$ and $|\phi_3\rangle$ are linearly dependent. We will consider the Bloch representation of quantum states. We can represent our SIC-POVM on the set of normalized Bloch vectors $B(3) \subset S^7$ (unit sphere) by the set of vertices of a regular 8-simplex, which we denote by $B := \{v_1, v_2, \ldots, v_9\}$. Inner products of vectors $\psi_1, \psi_2 \in \mathbb{C}^3$ and the corresponding normalized Bloch vectors $u_1, u_2 \in \mathbb{R}^8$ are related in the following way: $|\langle\psi_1|\psi_2\rangle|^2 = (2(u_1 \cdot u_2)+1)/3$ (see Sect. 1.3). In particular, if $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal, then $u_1 \cdot u_2 = -1/2$. Let us consider the five-dimensional affine subspace π_1:

$$\pi_1 := \{u \in \mathbb{R}^8 | u \cdot v_1 = u \cdot v_2 = u \cdot v_3 = -1/2\}$$

and the affine hyperplane π_2 tangent to the sphere S^7 at the point $w := -(v_1 + v_2 + v_3)/\|v_1 + v_2 + v_3\|$:

$$\pi_2 := \{w + u_0 | u_0 \in \mathbb{R}^8, u_0 \cdot w = 0\} = \{u \in \mathbb{R}^8 | u \cdot w = 1\}.$$

Taking into account that $v_i \cdot v_j = -1/8$ for $i \neq j$, and so $\|v_1 + v_2 + v_3\| = 3/2$ we get $w \in \pi_1 \subset \pi_2$. Thus w needs necessarily to be the Bloch vector corresponding to $|\psi\rangle$. For $j \in \{4, \ldots, 9\}$ we get $w \cdot v_j = 1/4$.

We now apply the method based on the Hermite interpolation described in details in Sect. 4.1.3. The function $H_B : B(d) \to \mathbb{R}^+$ defined in (40) now takes the form

$$H_B(u) := H(\rho, \Pi) = \sum_{j=1}^{9} \eta\left(\frac{2u \cdot v_j + 1}{9}\right) = \ln 3 + \frac{1}{3}\sum_{j=1}^{9} h(u \cdot v_j),$$

where u is the Bloch vector corresponding to $\rho \in \mathcal{P}(\mathbb{C}^d)$ and $h : [-1/2, 1] \to \mathbb{R}^+$ defined in (42) is now given by $h(t) = \eta\left(\frac{2t+1}{3}\right)$. We are looking for the interpolating Hermite polynomial p such that $p(-1/2) = h(-1/2)$, $p(1/4) = h(1/4)$ and $p'(1/4) = h'(1/4)$. What is crucial here is that again p interpolates h from below, see Observation 4.2 and subsequent remarks. The degree of p is at most 2, so it is the degree of the polynomial function $P : \mathbb{R}^8 \to \mathbb{R}$ given by $P(u) = \ln 3 + \frac{1}{3}\sum_{j=1}^{9} p(u \cdot v_j)$ for $u \in \mathbb{R}^8$. As $\sum_{j=1}^{9} v_j = 0$, the linear part vanishes. Additionally, since the vertices of a regular N-simplex in $\mathbb{R}^N$ form a tight frame in $\mathbb{R}^N$ with bound $N/(N-1)$, we get $\sum_{j=1}^{9} (u \cdot v_j)^2 = \frac{9}{8}\|u\|^2$ for any $u \in \mathbb{R}^8$. Hence P must be constant on any sphere. Using the fact that $P(u) \leq H_B(u)$ and $P(w) = H_B(w)$ we conclude that the entropy attains its minimum value (and so the relative entropy $\tilde{H}$ attains its maximum value) at $|\psi\rangle\langle\psi|$.

In order to show that all global minimizers of the entropy (and so maximizers of the relative entropy) are of the same form, i.e. they are orthogonal to some three out of nine vectors defining SIC-POVM, we use similar argument as in the last part of the proof of Theorem 4.5. In this way, we get that if $|\tilde{\psi}\rangle\langle\tilde{\psi}|$ is a global minimizer of the entropy, then $\{\tilde{w} \cdot v_j | j = 1, \ldots, 9\} \subset \{w \cdot v_j | j = 1, \ldots, 9\} =$

$\{-1/2, 1/4\}$, where $\tilde{w}$ is a normalized Bloch vector corresponding to $|\tilde{\psi}\rangle\langle\tilde{\psi}|$. Under the constraint $\sum_{j=1}^{9} \tilde{w} \cdot v_j = 0$ we get that $\{\tilde{w} \cdot v_j | j = 1, \ldots, 9\} = \{-1/2, 1/4\}$ and there are exactly three j's such that $\tilde{w} \cdot v_j = -1/2$, i.e. there are exactly three vectors $|\phi_j\rangle$ orthogonal to $|\tilde{\psi}\rangle$. $\square$

REMARK 4.2. Theorem 4.6 holds also if the Shannon entropy is replaced by the Rényi α-entropy or Havrda-Charvát-Tsallis α-entropy for $\alpha \in (0, 2)$. The reason is given in Remark 4.1.

Next theorem gives us a deeper insight into the algebraic structure of some entropy minimizers. The facts and notation from Sect. 2.4 are widely used.

THEOREM 4.7. *Let $(\mathcal{G}, \mathbf{q}) \in ESL(2, \mathbb{Z}_3) \ltimes (\mathbb{Z}_3)^2$ be such that $U_{(\mathcal{G},\mathbf{q})}$ is a canonical order 3 unitary conjugated (up to a phase in the extended Clifford group) to $U_{\mathcal{Z}}$. Then the relative entropy of 3-dimensional WH-covariant SIC-POVM, whose fiducial vector $|\phi_1\rangle$ is an eigenvector of $U_{(\mathcal{G},\mathbf{q})}$ is maximized in the eigenstates of Weyl matrix $D_{\mathbf{s}}$, where $\mathbf{s} \neq (0, 0)$ satisfies $\mathcal{G}\mathbf{s} = \mathbf{s}$.*

PROOF. It follows from Theorem 2.5 that operators $U_{(\mathcal{G},\mathbf{q})}$ and $U_{\mathcal{Z}}$ are conjugated if and only if $(\mathcal{G}, \mathbf{q})$ and $(\mathcal{Z}, 0)$ are conjugated, i.e. if and only if there exists $(\mathcal{F}, \mathbf{r}) \in \mathrm{ESL}(2, \mathbb{Z}_3) \ltimes (\mathbb{Z}_3)^2$ such that $\mathcal{G} = \mathcal{F}\mathcal{Z}\mathcal{F}^{-1}$ and $\mathbf{q} = (\mathcal{I} - \mathcal{G})\mathbf{r}$. Now, if $\mathbf{p}$ is a non-zero fixed point of $\mathcal{Z}$ (thus $\mathbf{p} = (1, 2)$ or $\mathbf{p} = (2, 1)$), then $\mathbf{s} = \mathcal{F}\mathbf{p}$ is a non-zero fixed point of $\mathcal{G}$. Let us observe that from (10) we get that $D_{\mathbf{s}}$ (and so $D_{\mathbf{s}}^2 = D_{2\mathbf{s}}$) commutes with $U_{(\mathcal{G},\mathbf{q})}$:

$$U_{(\mathcal{G},\mathbf{q})} D_{\mathbf{s}} = \omega^{\langle \mathbf{q}, \mathcal{G}\mathbf{s} \rangle} D_{\mathbf{s}} U_{(\mathcal{G},\mathbf{q})} = D_{\mathbf{s}} U_{(\mathcal{G},\mathbf{q})}, \tag{60}$$

since $\langle \mathbf{q}, \mathcal{G}\mathbf{s} \rangle = \langle \mathbf{r} - \mathcal{G}\mathbf{r}, \mathcal{G}\mathbf{s} \rangle = \langle \mathbf{r}, \mathbf{s} \rangle - \langle \mathcal{G}\mathbf{r}, \mathcal{G}\mathbf{s} \rangle = \langle \mathbf{r}, \mathbf{s} \rangle - \langle \mathbf{r}, \mathbf{s} \rangle = 0$. We consider the set S consisting of the vectors $|\phi_1\rangle$, $D_{\mathbf{s}}|\phi_1\rangle$ and $D_{2\mathbf{s}}|\phi_1\rangle$. By (60) they all belong to the same eigenspace of $U_{(\mathcal{G},\mathbf{q})}$. Since $U_{\mathcal{Z}}$ has two eigenspaces: one-dimensional and two-dimensional [**168**, Sect. 3.4], so has $U_{(\mathcal{G},\mathbf{q})}$ and we will refer to them by $\mathcal{H}_1$ and $\mathcal{H}_2$. Thus vectors from S must be linearly dependent, and since they are not colinear, they span $\mathcal{H}_2$. Let us take any $|\psi\rangle \in \mathcal{H}_1$. It is obviously orthogonal to the above vectors, and so from Theorem 4.6 we get that it maximizes the relative entropy of Π. There exists a common eigenbasis for $D_{\mathbf{s}}$ and $U_{(\mathcal{G},\mathbf{q})}$, thus $|\psi\rangle$ is also an eigenvector of $D_{\mathbf{s}}$. Since the entropy is a WH-invariant function and the orbit under the action of WH group of an eigenvector of $D_{\mathbf{s}}$ is an eigenbasis of this operator [**19**, Thm 2.2], the theorem is proven. $\square$

It is worth to notice that the above theorems are not equivalent, i.e. although Theorem 4.7 follows from Theorem 4.6, there may exist maximizers of the relative entropy that are not of the form indicated in Theorem 4.7. In consequence, the WH-covariant maximally informative ensemble (i.e. the maximally informative ensemble consisting of a single orbit of a maximizer of the relative entropy, see

Sect. 3.2) needs not necessarily form a single orthonormal basis (an eigenbasis of certain Weyl matrix), as the ensembles arising from Theorem 4.7 do.

Let us first recall that two orthonormal bases in $\mathbb{C}^d$, $\mathcal{B}_1 = \{|e_1\rangle, \ldots, |e_d\rangle\}$ and $\mathcal{B}_2 = \{|f_1\rangle, \ldots, |f_d\rangle\}$, are said to be *mutually unbiased* if $|\langle e_i|f_j\rangle|^2 = 1/d$ for $i, j = 1, \ldots, d$. The set $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of orthonormal bases in $\mathbb{C}^d$ is called a set of mutually unbiased bases (MUBs) if every two bases from this set are mutually unbiased.[3] Let us now consider a family of SIC-POVMs parametrized by $t \in [0, \pi/3]$ and generated by the following vectors: $(0, 1, -e^{it}\eta^j)$, $(-e^{it}\eta^j, 0, 1)$, $(1, -e^{it}\eta^j, 0)$, $j = 0, 1, 2$, where $\eta := e^{2\pi i/3}$. For every $t \in [0, \pi/3]$ the fiducial vector $|\phi_1\rangle := (0, 1, -e^{it})$ is an eigenvector of unitary $U_{(\mathcal{G},0)}$ for $\mathcal{G} = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Thus, according to Theorem 4.7, $|\phi_1\rangle, D_{\mathbf{s}}|\phi_1\rangle$ and $D_{\mathbf{s}}^2|\phi_1\rangle$, where $\mathbf{s} := (0, 1)$ is a fixed point of $\mathcal{G}$, are linearly dependent and the maximal relative entropy is attained in the eigenstates of operator $D_{\mathbf{s}}$. In consequence, a WH-covariant maximally informative ensemble consists of the eigenbasis of $D_{\mathbf{s}}$. Nevertheless, there are two special cases: $t = 0$ and $t = 2\pi/9$, described in details in [**50**, Sect. 3]. In the former, $|\phi_1\rangle$ is an eigenvector of every *symplectic* canonical order 3 unitary (i.e. one of the form $U_{(\mathcal{F},0)}$). It is easy to check that for every $\mathbf{r} \in \mathbb{Z}_3$ there exists $\mathcal{F} \in \mathrm{ESL}(2, \mathbb{Z}_3)$ such that $\mathcal{F}\mathbf{r} = \mathbf{r}$ and $U_{(\mathcal{F},0)}$ is a canonical order 3 unitary, and so, by Theorem 4.7, the maximal relative entropy is attained at the eigenstates of any Weyl matrix. Thus the maximizers form a set of four MUBs (mutually unbiased bases) [**19**, Thm 2.3] and there are four WH-covariant maximally informative ensembles, each consisting of different eigenbases of Weyl matrices. In the latter case, we get additional linear dependencies that do not arise from the eigenspace of any canonical order 3 unitary[4], e.g. between vectors $|\phi_1\rangle, D_{(1,2)}|\phi_1\rangle$ and $D_{(2,0)}|\phi_1\rangle$. It turns out that the orbit under the action of WH group of the vector orthogonal to one of these additional subspaces consists of three MUBs and together with the maximizers described in Theorem 4.7 they form a set of four MUBs. Therefore there are two WH-covariant maximally informative ensembles: one consisting of eigenbasis of $D_{\mathbf{s}}$ and second one consisting of three MUBs indicated above.

---

[3]The existence of maximal set of mutually unbiased bases in $\mathbb{C}^d$ (i.e. consisting of $d + 1$ MUBs) for arbitrary d is an open problem of similar complexity as the existence of SIC-POVMs in any dimension, see [**4**]. While the Bloch representation of a SIC-POVM consists of vertices of regular $(d^2 - 1)$-simplex inscribed into $(2d - 2)$-dimensional set of Bloch vectors, the Bloch representation of $d+1$ MUBs forms $d+1$ mutually orthogonal (see (5)) regular $(d-1)$-simplices inscribed into the same set. However, the existence of full set of MUBs has been already confirmed for dimensions that are primes [**92**] or powers of primes [**19**]. Moreover, it is believed that set of $d+1$ MUBs does not exist for every d, e.g. for $d = 6$ the maximal sets of MUBs that have been found so far consist of 3 MUBs and there is a numerical evidence that there are no more of them [**37**].

[4]It follows from the fact that no other canonical order 3 unitaries stabilize $|\phi_1\rangle$ for $t > 0$.

4.5. Pure states of maximal entropy

The entropy of rank-1 normalized POVM $\Pi = \{\Pi_j\}_{j=1}^k$ is obviously maximal for maximally mixed state $\rho_* = (1/d)\mathbb{I}$ since then $\mathrm{Tr}(\rho_*\Pi_j) = (1/d)\mathrm{Tr}(\Pi_j) = (1/d)(d/k) = 1/k$, i.e. the measurement outcomes are uniformly distributed. However, if we consider the entropy of the measurement restricted to the pure states, the question, which pure states maximize the entropy of the measurement and how large can it be, is not so trivial. Before we start to analyze the answer, let us ask, what is the meaning of this question? Let us observe that since the entropy is minimized on the set of pure states, one can ask, how badly can we end by choosing initially any pure state.

While stating the problem of minimization of the entropy of POVM we said that we are looking for the states that are most classical (with reference to a given POVM). Thus the question set above may be interpreted as asking which pure states are most quantum with respect to a given POVM. Similar problems, concerning the maximal 'quantumness', has been already stated in the context of coherent states. Giraud et al. [**71**] analyzed the quantity defined as the Hilbert-Schmidt distance between a given state and the convex hull of coherent states, while Bæcklund and Bengtsson [**15, 16**] addressed the problem of the Wehrl entropy maximization (see Sect. 3.3). Interestingly, the solutions for both problems, poetically called by the authors of [**71**] 'Queens of Quantum', coincide for dimensions from two to eight and ten, but not for nine (higher dimensional cases have not been considered yet).

Let us recall that by (16) the maximization of the entropy H over pure states is equivalent to the minimization of the relative entropy $\widetilde{H}$ over pure states, which, in general, is always minimal and equal 0 for maximally mixed state ρ_*. We found it more convenient to express the following claims in terms of relative entropy.

FACT 4.1.
1. If the rank-1 normalized $\Pi = \{\Pi_j\}_{j=1}^k$ is informationally complete, then
$$\min_{\rho \in \mathcal{P}(\mathbb{C}^d)} \widetilde{H}(\rho, \Pi) > 0. \tag{61}$$
Moreover, if $d = 2$, the converse is also true.
2. If Π is a PVM, then $\min\limits_{\rho \in \mathcal{P}(\mathbb{C}^d)} \widetilde{H}(\rho, \Pi) = 0$.

PROOF.

1. If $\widetilde{H}(\rho, \Pi) = 0$, then $H(\rho, \Pi) = \ln k$, and so the probability distribution of the measurement outcomes is uniform. By the informational completeness of Π we get that $\rho = \rho_*$ and so $\min_{\rho \in \mathcal{P}(\mathbb{C}^d)} \widetilde{H}(\rho, \Pi) > 0$.

Now let $d = 2$. To see the converse, let us assume that Π is not informationally complete. Then, by Proposition 2.3 and the fact that $b(\mathcal{P}(\mathbb{C}^2))$ is the unit sphere in $\mathcal{L}_s^0(\mathbb{C}^2)$ (see Sect. 1.3), there exists $\sigma \in \mathcal{P}(\mathbb{C}^2)$ such that $\langle\langle b(\sigma), b(\rho_j)\rangle\rangle_{HS} = 0$

for $j = 1, \ldots, k$, where ρ_j is a pure state corresponding to Π_j. In consequence, $\mathrm{Tr}(\sigma\Pi_j) = 1/k$ for all j and $\widetilde{H}(\sigma, \Pi) = 0$.

2. If Π is a PVM, i.e. $\Pi := \{|e_j\rangle\langle e_j|\}_{j=1}^d$, where $\{|e_j\rangle\}_{j=1}^d$ is an orthonormal basis in $\mathbb{C}^d$, then the uniform distribution of the measurement outcomes appears for any initial state $|\psi\rangle\langle\psi|$ of the form $|\psi\rangle = (1/\sqrt{d})\sum_{j=1}^d e^{i\theta_j}|e_j\rangle$, where $\theta_j \in \mathbb{R}$. $\square$

Let us remind that in Sect. 4.1.5 we have already made a remark about the states of maximal entropy in the case of rank-1 normalized POVMs on $\mathbb{C}^2$, whose Bloch representation is two-dimensional.

An obvious question that arises here is whether we can compute exact values of the maximum entropy H, i.e. the minimum relative entropy $\widetilde{H}$ for at least some classes of POVMs. Firstly, we claim that the minimum relative entropy of a SIC-POVM is always attained at the states constituting this SIC-POVM:

THEOREM 4.8. *Let $\Pi = \{(1/d)|\phi_j\rangle\langle\phi_j|\}_{j=1}^{d^2}$ be a SIC-POVM in dimension d. Then states $|\phi_j\rangle\langle\phi_j|$ for $j = 1, \ldots, d^2$ are the only minimizers of the relative entropy restricted to the pure states and*

$$\min_{\rho\in\mathcal{P}(\mathbb{C}^d)} \widetilde{H}(\rho, \Pi) = \widetilde{H}(|\phi_j\rangle\langle\phi_j|, \Pi) = \ln d - \frac{d-1}{d}\ln(d+1), \tag{62}$$

for $j = 1, \ldots, d^2$. Moreover, $\min_{\rho\in\mathcal{P}(\mathbb{C}^d)} \widetilde{H}(\rho, \Pi) \xrightarrow{d\to\infty} 0$.

PROOF. From (9) we obtain $p_i(|\phi_j\rangle\langle\phi_j|, \Pi) = \mathrm{Tr}((1/d)|\phi_j\rangle\langle\phi_j|\phi_i\rangle\langle\phi_i|) = 1/(d(d+1))$ for $i \neq j$ and $p_j(|\phi_j\rangle\langle\phi_j|, \Pi) = 1/d$. Thus we get the second equality in (62). To see that it is indeed the minimum value of the relative entropy on $\mathcal{P}(\mathbb{C}^d)$, let us use again the Hermite interpolation method, see Sect. 4.1.3. We use the entropy of Π redefined in (40) to be a function of Bloch vectors, that now takes the following form:

$$H_B(u) := H(\rho, \Pi) = \sum_{j=1}^{d^2} \eta\left(\frac{(d-1)u\cdot v_j + 1}{d^2}\right) = \ln d + \frac{1}{d}\sum_{j=1}^{d^2} h(u\cdot v_j),$$

where $u, v_1, \ldots, v_{d^2}$ are the Bloch vectors corresponding to $\rho, |\phi_1\rangle\langle\phi_1|, \ldots, |\phi_{d^2}\rangle\langle\phi_{d^2}|$, and $h : [-1/(d-1), 1] \to \mathbb{R}^+$, defined in (42), is given by $h(t) := \eta\left(\frac{(d-1)t+1}{d}\right)$ for $t \in [-1/(d-1), 1]$. Since $-1/(d-1)$ does not belong to the set of points of interpolation $T := \{-1/(d^2-1), 1\}$, the interpolating Hermite polynomial p such that $p(1) = h(1)$, $p(-1/(d^2-1)) = h(-1/(d^2-1))$ and $p'(-1/(d^2-1)) = h'(-1/(d^2-1))$ interpolates h from above, see Observation 4.2 and subsequent remarks. Thus the polynomial function given by $P(u) := \ln d + \frac{1}{d}\sum_{j=1}^{d^2} p(u\cdot v_j)$ for $u \in B(d)$ is of degree less than 3. Since every SIC-POVM is a projective 2-design, P is necessarily constant on the whole Bloch set. Using the fact that $P(u) \geq H_B(u)$ and $P(v_j) = H_B(v_j)$ for $j = 1, \ldots, d^2$, we conclude that the entropy attains its maximum (and so the relative entropy – minimum) value on the set of pure states at $|\phi_j\rangle\langle\phi_j|$ ($j = 1, \ldots, d^2$).

Using similar argument as in the last part of the proof of Theorem 4.5, we get that if a pure state ρ is also a global maximizer of the entropy, then $\{u \cdot v_j | j = 1, \ldots, d^2\} \subset T = \{-1/(d^2-1), 1\}$, where u is a normalized Bloch vector corresponding to ρ. Using the fact that $\sum_{j=1}^{d^2} u \cdot v_j = 0$, we get that $\{u \cdot v_j | j = 1, \ldots, d^2\} = T$, and so $u \in \{v_1, \ldots, v_{d^2}\}$. Thus the uniqueness is proven. The limit as $d \to \infty$ follows from direct calculation. □

The following theorem provides the global minimizers of the relative entropy of informationally complete HS-POVMs in dimension two. All of them has been already indicated as local minimizers in Proposition 4.4. However, not all local minimizers found there turn out to be the global ones, see the cuboctahedral and icosidodecahedral case.

THEOREM 4.9. *Let Π be an informationally complete HS-POVM in dimension two, but not a SIC-POVM*[5]*. Then the entropy (resp. relative entropy) of Π restricted to the set of pure states attains its maximum (resp. minimum) value exactly in the states which Bloch vectors correspond to*

1) the vertices of the dual polyhedron, if Π is represented by a platonic solid,
2) the vertices of the octahedron, if Π is represented by cuboctahedron,
3) the vertices of the icosahedron, if Π is represented by icosidodecahedron.

PROOF. We proceed in a similar way as in the proof of Theorem 4.5, interpolating function $h : [-1, 1] \to \mathbb{R}^+$ defined by (42). The set of interpolating points is defined by $T := \{w \cdot u | u \in Gv\}$, where v is the Bloch vector of the fiducial state and w is the Bloch vector indicated in the theorem's statement. Note that $T \subset (-1, 1)$, and thus, after choosing the interpolating polynomial to agree with h in every $t \in T$ up to the first derivative, we get that p_v interpolates h from above and $\deg p_v < 2|T|$, see Fig. 5. Thus, it is enough to show that the polynomial P_v given by $P_v(u) := \ln(|G|/2) + (2/|G|) \sum_{g \in G} p_v(u \cdot gv)$ for $u \in B(2)$ attains its maximum value in the orbit of w. Note that in case 1) we get the same polynomials p_{v_1} and p_{v_2} for dual POVMs (the sets of interpolating points coincide), but P_{v_1} and P_{v_2} differ. Throughout the proof we shall frequently use the fact that P_v is G-invariant and so can be expressed in terms of primary invariants, see Sect. 4.1.4, especially Tab. 2.

Cube and **octahedron.** This case is straightforward, as $|T| = 2$, the degree of the interpolating polynomial is at most 3, and so both P_{v_1} and P_{v_2} need to be constant on the sphere.

Icosahedron and **dodecahedron.** In this cases we have $|T| = 4$ and $\deg p_{v_1} = \deg p_{v_2} \leq 7$. In consequence, $P_{v_1}|_{S^2} = A_1 + B_1 I_6'$ and $P_{v_2}|_{S^2} = A_2 + B_2 I_6'$

[5]That is, we exclude here the tetrahedral case covered already by Theorem 4.8.

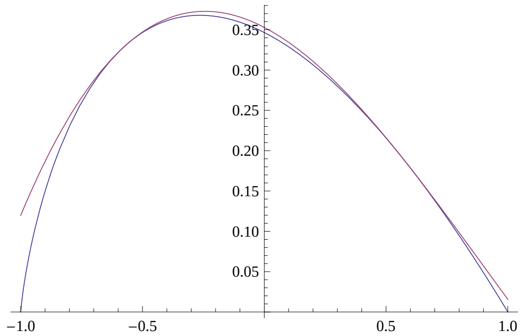

FIGURE 5. The cubic polynomial function p_v (*purple*) interpolating h (*violet*) from above for the octahedral and cubic measurements, with $t_1 = -1/\sqrt{3}$ and $t_2 = 1/\sqrt{3}$.

for some $A_1, A_2, B_1, B_2 \in \mathbb{R}$. Thus it suffices to show that $B_1 > 0$ and $B_2 < 0$. We find their values as previously, by calculating P_v in two chosen points from different orbits and check that they are indeed of desired sign.

Cuboctahedron. For the cuboctahedral measurement we get $|T| = 3$ and $\deg P_v \leq \deg p_v \leq 5$. Thus $P_v|_{S^2} = A + BI_4$ for some $A, B \in \mathbb{R}$. Proceeding as in the previous case, we find the value of B and check that it is positive.

Icosidodecahedron. In this case we get $|T| = 5$ and so $\deg P_v \leq \deg p_v \leq 9$. In consequence, $P_v|_{S^2} = A + BI_6'$ for some $A, B \in \mathbb{R}$. Again, we calculate B using the same method as before and check that it is negative.

To see the uniqueness of given global maximizers of the entropy we use similar argument as in the last part of the proof of Theorem 4.5 to get that if a pure state ρ is also a global maximizer of the entropy, then $\{\tilde{w} \cdot u | u \in Gv\} \subset T$, where $\tilde{w}$ is a normalized Bloch vector corresponding to ρ. Using the fact that $\sum_{u \in Gv} \tilde{w} \cdot u = 0$ and $\sum_{u \in Gv} (\tilde{w} \cdot u)^2 = |Gv|/3$ (as Gv is 2-design) we get not only that $\{\tilde{w} \cdot u | u \in Gv\} = T$, but also the multiplicities of the elements need to agree. It is easy to see that there are no other vectors in S^2 with this property. $\square$

4.6. Remarks on alternative proofs for some cases

In the thesis we presented a universal method of determining the global extrema of the entropy of POVM. However, in some cases it is possible to give proofs that appear to be more elementary. We discuss them below.

REMARK 4.3. It is possible to complete the proof of Theorem 4.6 in another way, starting from the point that the input state $|\psi\rangle\langle\psi|$ gives the probability distribution $(0, 0, 0, 1/6, \ldots, 1/6)$. It is enough to notice that the lower bound for the Shannon entropy, namely $\ln 6$, provided by Rastegin [**125**, Prop. 6] is satisfied here, as it was done in [**13**, Corol. 2]. Moreover, this reasoning applies also to some generalized entropies as it turns out that both the lower bounds, i.e.

$(1-\alpha)^{-1}(6^{1-\alpha}-1)$, for Havrda-Charvát-Tsallis α-entropies for $\alpha \in (0,2]$ given in [**125**, Prop. 6], as well as the lower bound $\ln 6$ for Rényi α-entropies for $\alpha \in (0,2]$, given in [**125**] as the corollary from Prop. 7, are achieved. However, the dimension three can be exceptional, in the sense that the lower bounds obtained in [**125**] may not be satisfied in higher dimensions, as indicated by some preliminary numerical calculations in dimensions four to six.[6] The possible reason will be lightened in the next remark. On the other hand, the method based on the Hermite interpolation seems to be applicable also in the higher dimensions.

REMARK 4.4. Let us recall that for tight informationally complete POVMs the sum of squared probabilities of the measurement outcomes (known as the *index of coincidence*) is the same for each initial pure state and equal to $2d/(k(d+1))$. The problem of finding the minimum and maximum of the Shannon entropy under assumption that the index of coincidence is constant has been analyzed in [**82**] (some generalizations and related topics can be found also in [**25, 174**]). By [**82**, Thm 2.5.] we get that the minimum is achieved for the probability distribution $(p,\ldots,p,q,0,\ldots,0)$, where there are $\lfloor k(d+1)/(2d) \rfloor$ probabilities equal to p, and both p and q are uniquely determined by the value of the index of coincidence. On the other hand, the maximum is attained for the probability distribution of the form $(p,q,\ldots,q)$, where $q = (1-\sqrt{(d-1)/((d+1)(k-1))})/k$ and $p = 1-(k-1)q$.

One would not suppose this fact to be useful in general setting, since the possible probability distributions of the measurement outcomes for initial pure states form just a $(2d-2)$-dimensional subset of a $(k-2)$-dimensional intersection of a $(k-1)$-sphere and the simplex Δ_k. As $2d < k$, unless $d = 2$ and $k = 4$,[7] so, in general situation, these extremal points need not necessarily belong to it. However, this method can be applicable in some cases:

(1) Global minimizers for SIC-POVMs in dimensions two and three (Theorem 4.5 – tetrahedral case, Theorem 4.6): the probability distributions for the states claimed to minimize the entropy of measurement are of the form $(1/3,1/3,1/3,0)$ and $(1/6,1/6,1/6,1/6,1/6,1/6,0,0,0)$.
(2) Global maximizers for SIC-POVMs in arbitrary dimension d (Theorem 4.8): the probability distributions for the states claimed to maximize the entropy of measurement are of the form $(1/d, 1/(d(d+1)),\ldots,1/(d(d+1)))$.

The natural question that arise now is whether case (1) could be generalized to higher dimensions. Let us observe that the demanded probability distribution should be then of the form $(2/(d(d+1)),\ldots,2/(d(d+1)),0,\ldots,0)$ with $d(d-1)/2$

[6]The numerical calculations has been done with *Mathematica* standard commands. Various methods has been tested, including ‘simulated annealing’. Independently, numerical research in dimension four has been made also by Dall’Arno et al. [**13**, Sect. 4].

[7]If Π is informationally complete, then $k \geq d^2$, see p. 23.

zeros. It means that among the state vectors defining a SIC-POVM there should exist $d(d-1)/2$ vectors that span at most $(d-1)$-dimensional subspace. This does not sound to be highly probable, or, at least, it would be hard to expect such pattern to arise from the WH-covariance, as in dimension three, see [**50**]. Note that the bounds given by Rastegin [**125**], see Remark 4.3, are exactly the same as those which can be delivered from the above probability distribution.

However, for SIC-POVM $\{\Pi_j\}_{j=1}^{d^2}$ there exists additional constraint on the set of 'allowed' probabilities, namely

$$\sum_{j_1,j_2,j_3=1}^{d^2} c_{j_1j_2j_3} p_{j_1} p_{j_2} p_{j_3} = \frac{d+7}{(d+1)^3}, \tag{63}$$

where $c_{j_1j_2j_3} := \Re(\mathrm{Tr}(\Pi_{j_1}\Pi_{j_2}\Pi_{j_3}))$, $p_{j_i} := \mathrm{Tr}(\rho\Pi_{j_i})$ for $i=1,2,3$ and $\rho \in \mathcal{P}(\mathbb{C}^d)$. The probability distributions fulfilling (63) together with the constraint on the sum of squared probabilities provide full characterization of the set of 'allowed' probabilities [**7**]. One can hope that this description may be used to solve the minimization entropy problem for SIC-POVMs in certain dimensions higher than three.

Another question one can ask here is whether it is possible to derive a proof of Theorem 4.5 for HS-POVMs with octahedral and icosahedral symmetry using the fact that the corresponding Bloch vectors are spherical 3-designs and 5-designs, respectively. The question consists of two problems. The first one is to find the probability distributions that minimize Shannon entropy under assumption that Rényi α-entropies are fixed for $\alpha = 2,3$ and $\alpha = 2,3,4,5$, respectively. The second one is whether the obtained extremal probability distribution belongs to the 'allowed' set, as the conditions on Rényi entropies do not give a complete characterization of this set.

4.7. Informational power and the average value of relative entropy

While we know the minimum and maximum values of the relative entropy of some POVMs, it would be worth taking a look at its average. Surprisingly, the average value of relative entropy over all pure states does not depend on the measurement Π, but only on the dimension d. This can be proved using (24) and the formula (21) from Jones [**94**]. Namely, we have

$$\begin{aligned}\left\langle \widetilde{H}(\rho,\Pi)\right\rangle_{\rho\in\mathcal{P}(\mathbb{C}^d)} &= \int_{\mathcal{P}(\mathbb{C}^d)} \left(\ln d - \frac{d}{k}\sum_{j=1}^{k} \eta\left(\mathrm{Tr}\left(\rho\rho_j\right)\right)\right) \mathrm{d}m_{FS}(\rho) \\ &= \ln d - d\left(\int_{\mathcal{P}(\mathbb{C}^d)} \eta\left(\mathrm{Tr}\left(\rho\rho_1\right)\right) \mathrm{d}m_{FS}(\rho)\right) \\ &= \ln d - \sum_{j=2}^{d}\frac{1}{j} \to 1-\gamma \quad (d\to\infty),\end{aligned} \tag{64}$$

where $\gamma \approx 0.57722$ is the Euler-Mascheroni constant. This average is also equal to the maximum value (in dimension d) of entropy-like quantity called *subentropy*, providing the lower bound for accessible information [**96, 51**].

In particular, the average value of relative entropy is the same for every HS-POVM Π in dimension two and equals $\ln 2 - 1/2 \approx 0.19315$. It follows from Theorem 4.5 and (44) that its maximal value, that is the informational power of Π, is given by the formula

$$W(\Pi) = \ln 2 - \frac{2}{|G/G_v|} \sum_{[g] \in G/G_v} \eta\left(\frac{1 - gv \cdot v}{2}\right), \tag{65}$$

where G is any group acting transitively on the set of Bloch vectors representing Π. Recall that the number of different summands in (65) is bounded by the number of self-inverse double cosets of G_v plus half of the number of non self-inverse ones.

Applying the above formula to the n-gonal POVM we get

$$W(\Pi) = \ln 2 - \frac{2}{n} \sum_{j=1}^{n} \eta\left(\sin^2 \frac{\pi j}{n}\right) \to 1 - \ln 2 \approx 0.30685 \ (n \to \infty). \tag{66}$$

The approximate values of informational power for other HS-POVMs in dimension two as well as the minimum relative entropy on pure states computed in Sect. 4.5 can be found in Tab. 5.

convex hull of the orbit	informational power (max relative entropy)	min relative entropy
digon	0.69315	0
regular n-gon ($n \to \infty$)	0.30685	0
tetrahedron	0.28768	0.14384
octahedron	0.23105	0.17744
cube	0.21576	0.17744
cuboctahedron	0.20273	0.18443
icosahedron	0.20189	0.18997
dodecahedron	0.19686	0.18997
icosidodecahedron	0.19486	0.19099
average relative entropy	0.19315	

TABLE 5. The approximate values of informational power (maximum relative entropy) and minimum relative entropy on pure states (up to five digits) for all types of HS-POVMs in dimension two.

Comparing these values to the average value of relative entropy, we see that the larger is the number of elements in the HS-POVM, the flatter is the graph of $\widetilde{H}$; see also Fig. 6, where the graphs in spherical coordinates are presented.

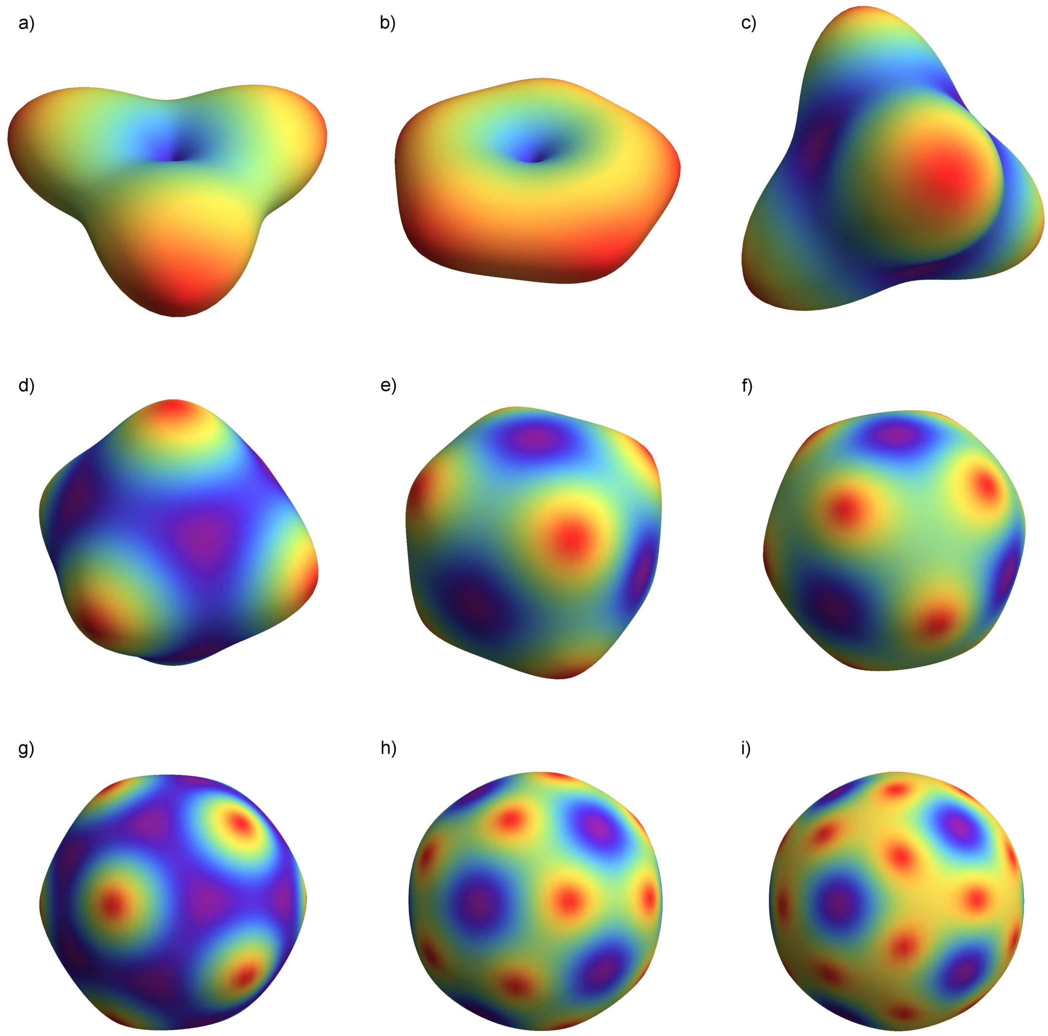

FIGURE 6. The relative entropy of highly symmetric qubit measurements, where their Bloch vectors form: a) an equilateral triangle; b) a regular pentagon; c) a tetrahedron; d) an octahedron; e) a cube; f) a cuboctahedron; g) an icosahedron; h) a dodecahedron; i) an icosidodecahedron. The rainbow-colors scale that ranges from *red* (maximum) to *purple* (minimum) is used.

Now let us take a closer look at SIC-POVMs. Although we are able to calculate the values of informational power only in dimensions two and three, we can use for higher dimensions the upper bounds provided in [**13**] equal $\ln(2d/(d+1))$. The minimum relative entropy on pure states is given by (62). The approximate values of all these quantities can be found in Tab. 6. The graph showing how the values change as the dimension grows is presented in Fig. 7.

dimension	informational power (upper bound)	average value of relative entropy	min relative entropy
2	0.28768	0.19315	0.14384
3	0.40547	0.26528	0.17442
4	0.47000	0.30296	0.17922
5	0.51083	0.32611	0.17603
6	0.53900	0.34176	0.17017
d	$\ln \frac{2d}{d+1}$	$\ln d - \sum_{j=2}^{d} \frac{1}{j}$	$\ln d - \frac{d-1}{d} \ln(d+1)$
$d \to \infty$	$\ln 2 \approx 0.69315$	$1 - \gamma \approx 0.42278$	0

TABLE 6. The approximate values of informational power (upper bounds for $d > 3$), average and minimum relative entropy on pure states (up to five digits) for SIC-POVMs.

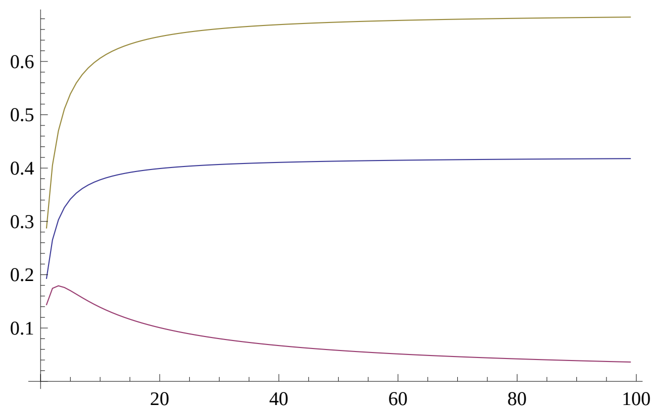

FIGURE 7. The upper bound for informational power (*dark yellow*), average value of relative entropy (*violet*) and minimum relative entropy on pure states (*purple*) of SIC-POVMs in dimensions from 2 to 100.

Let us observe that, although both the average and minimum value of the relative entropy of a SIC-POVM depend only on the dimension d, as it was shown in this thesis, it is hard to say whether the informational power behaves in the same way. The main problem is that we still know very little about SIC-POVMs in general. It is not only the problem of their existence in every dimension that is the most important here, but also how many of them (that are not unitarily equivalent) there exist in a given dimension. Hopefully, the methods developed in this thesis will help to overcome these obstacles.

Bibliography

[1] Ali, S.T., Antoine, J.P., Gazeau, J.-P.: Coherent States, Wavelets and Their Generalizations. Springer, New York (2014)

[2] Andreev, N.: Minimum potential energy of a point system of charges (Russian). Tr. Mat. Inst. Steklova **219**, 27–31 (1997); transl. in Proc. V.A. Steklov Inst. Math. **219**, 20–24 (1997)

[3] Appleby, D.M.: Symmetric informationally complete-positive operator valued measures and the extended Clifford group. J. Math. Phys. **46**, 052107 (2005)

[4] Appleby, D.M.: *SIC-POVMs and MUBs: Geometrical relationships in prime dimensions.* In: Accardi, L. et al. (eds.) Proceedings of the Växjö Conference on Foundations of Probability and Physics – 5, pp. 223–232. AIP, New York (2009)

[5] Appleby, D.M., Bengtsson, I., Brierley, S., Grassl, M., Gross, D., Larsson, J.-Å.:The monomial representations of the Clifford group. Quantum Inf. Comput. **12**, 0404–0431 (2012)

[6] Appleby, D.M., Bengtsson, I., Brierley, S., Ericsson, Å., Grassl, M., Larsson, J.-Å.: Systems of imprimitivity for the Clifford group. Quantum Inf. Comput. **14**, 339–360 (2014)

[7] Appleby, D.M., Dang, H.B., Fuchs, C.A.: Symmetric informationally-complete quantum states as analogues to orthonormal bases and minimum-uncertainty states. Entropy **16**, 1484–1492 (2014)

[8] Appleby, D.M., Ericsson, Å., Fuchs, C.A.: Properties of QBist state spaces. Found. Phys. **41**, 564–579 (2011)

[9] Appleby, D.M., Fuchs, C.A., Zhu, H.: Group theoretic, Lie algebraic and Jordan algebraic formulations of the SIC existence problem. arXiv:1312.0555 [quant-ph]

[10] D'Ariano, G.M., Perinotti, P., Sacchi, M.F.: Informationally complete measurements and groups representation. J. Opt. B **6**, S487–S491 (2004)

[11] Dall'Arno, M., D'Ariano, G.M., Sacchi, M.F.: Informational power of quantum measurement. Phys. Rev. A **83**, 062304 (2011)

[12] Dall'Arno, M., D'Ariano, G.M., Sacchi, M.F.: How much a Quantum Measurement is Informative? Preprint.

[13] Dall'Arno, M., Buscemi, F., Ozawa, M.: Tight bounds on accessible information and informational power. J. Phys. A **47** 235302 (2014)

[14] Arrighi, P., Patricot, C.: The conal representation of quantum states and non trace-preserving quantum operations. Phys. Rev. A **68**, 042310 (2003)

[15] Bæcklund, A.: *Maximization of the Wehrl Entropy in Finite Dimensions* MSc Thesis, KTH (2013) *available online at* http://www.kiko.fysik.su.se/en/thesis/AnnaWehrl.pdf

[16] Bæcklund, A., Bengtsson, I.: Four remarks on spin coherent states. arXiv:1312.2427 [quant-ph]

[17] Balian, R., Vénéroni, M., Balazs, N.: Relevant entropy *vs.* measurement entropy. Europhys. Lett. **1**, 1–5 (1986)

[18] Bandyopadhyay, J.: Optimal concentration for $SU(1,1)$ coherent state transforms and an analogue of the Lieb-Wehrl conjecture for $SU(1,1)$. Comm. Math. Phys. **285**, 1065–1086 (2009)

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

[20] Basu, S., Pollack, R., Roy, M.-F.: Algorithms in Real Algebraic Geometry, 2nd ed. Springer, Berlin (2006)

[21] Beck, C., Graudenz, D.: Symbolic dynamics of successive quantum-mechanical measurements. Phys. Rev. A **46**, 6265–6276 (1992)

[22] Benedetto, J.J., Fickus, M.: Finite normalized tight frames. Adv. Comput. Math. **18**, 357–385 (2003)

[23] Bengtsson, I., Weis, S., Życzkowski, K.: *Geometry of the Set of Mixed Quantum States: An Apophatic Approach.* In: Kielanowski, P., Ali, S.T., Odzijewicz, A., Schlichenmaier, M., Voronov, T. (eds.) Geometric Methods in Physics. XXX Workshop 2011, Trends in Mathematics, pp. 175–197. Springer, Basel (2013)

[24] Bengtsson, I., Życzkowski, K.: Geometry of Quantum States: an Introduction to Quantum Entanglement. Cambridge UP, Cambridge (2006)

[25] Berry, D.W., Sanders, B.C.: Bounds on general entropy measures. J. Phys. A **36**, 12255 (2003)

[26] Bertlmann, R.A., Krammer, P.: Bloch vectors for qudits. J. Phys. A **41**, 235303 (2008)

[27] Białynicki-Birula, I., Mycielski, J.: Uncertainty relations for information entropy in wave mechanics. Comm. Math. Phys. **44**, 129–132 (1975)

[28] Bogopolski, O.: Introduction to Group Theory. European Mathematical Society, Zürich (2008)

[29] Bosyk, G.M., Portesi, M., Plastino, A.: Collision entropy and optimal uncertainty. Phys. Rev. A **85**, 012108 (2012)

[30] Broome, H.: Highly symmetric tight frames (Honours project report). University of Auckland (2010)

[31] Broome, H., Waldron, S.: On the construction of highly symmetric tight frames and complex polytopes. Linear Algebra Appl. **439**, 4135–4151 (2013)

[32] de Burgh, M.D., Langford, N.K., Doherty, A.C., Gilchris, A.: Choice of measurement sets in qubit tomography. Phys. Rev. A **78**, 052122 (2008)

[33] Busch, P.: Informationally complete sets of physical quantities. Int. J. Theor. Phys. **30**, 1217–1227 (1991)

[34] Busch, P., Grabowski, M., Lahti, P.J.: Operational Quantum Physics. Springer-Verlag, Berlin (1995)

[35] Busch, P., Schonbek, T.P., Schroeck, Jr., F.E.: Quantum observables: Compatibility versus commutativity and maximal information. J. Math. Phys. **28**, 2866–2872 (1987)

[36] Busch, P., Schroeck, Jr., F.E.: On the reality of spin and helicity. Found. Phys. **19**, 807–872 (1989)

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

[38] Cabello, A.: Kochen-Specker theorem for a single qubit using positive operator-valued measures. Phys. Rev. Lett. **90**, 190401 (2003)

[39] Casazza, P.G., Kutyniok, G., Philipp, F.: *Introduction to Finite Frame Theory.* In: Casazza, P.G., Kutyniok, G. (eds.) Finite Frames. Theory and Applications, pp. 1–53. Birkhäuser, Basel (2013)

[40] Cassinelli, G., De Vito, E., Lahti, P.J., Levrero, A.: Symmetry groups in quantum mechanics and the theorem of Wigner on the symmetry transformations. Rev. Math. Phys. **9**, 921–941 (1997)

[41] Cassinelli, G., De Vito, E., Lahti, P.J., Levrero, A.: The Theory of Symmetry Actions in Quantum Mechanics. Springer, Berlin (2003)

[42] Caves, C.M., Fuchs, C.A., Manne, K.K., Renes, J.M.: Gleason-type derivations of the quantum probability rule for generalized measurements. Found. Phys. **34**, 193–209 (2004)

[43] Cohn, H., Kumar, A.: Universally optimal distribution of points on spheres. J. Amer. Math. Soc. **20**, 99–148 (2007)

[44] Cohn, H., Woo, J.: Three-point bounds for energy minimization. J. Amer. Math. Soc. **25**, 929–958 (2012)

[45] Coles, P.J., Yu, L., Gheorghiu, V., Griffiths, R.B.: Information-theoretic treatment of tripartite systems and quantum channels. Phys. Rev. A **83**, 062338 (2011)

[46] Crann, J., Pereira, R., Kribs, D.W.: Spherical designs and anticoherent spin states. J. Phys. A **43**, 255307 (2010)

[47] Cromwell, P.R.: Polyhedra. Cambridge UP, Cambridge (1997)

[48] Crutchfield, J.P., Wiesner, K.: Intrinsic quantum computation. Phys. Lett. A **372**, 375–380 (2008)

[49] Csiszár, I.: Axiomatic characterizations of information measures. Entropy **10**, 261–273 (2008)

[50] Dang, H.B., Blanchfield, K., Bengtsson, I., Appleby, D.M.: Linear dependencies in Weyl-Heisenberg orbits. Quantum Inf. Process. **12**, 3449–3475 (2013)

[51] Datta, N., Dorlas, T., Jozsa, R., Benatti, F.: Properties of subentropy. arXiv:1310.1312 [quant-ph].

[52] Davies, E.B.: Quantum Theory of Open Systems. Academic Press, New York (1976)

[53] Davies, E.B.: Information and quantum measurement. IEEE Trans. Inf. Theory **24**, 596–599 (1978)

[54] Davies, E.B., Lewis, J.: An operational approach to quantum probability. Comm. Math. Phys. **17**, 239–260 (1970)

[55] Decker, T., Grassl, M.: *Implementation of Generalized Measurements with Minimal Disturbance on a Quantum Computer.* In: Schleich, W.P., Walther, H. (eds.): Elements of Quantum Information, pp. 399–424. Wiley-VCH, Weinheim (2007)

[56] Decker, T., Janzing, D., Beth, T.: Quantum circuits for single-qubit measurements corresponding to platonic solids. Int. J. Quantum Inform. **2**, 353–378 (2004)

[57] Delsarte P., Goethals, J.M., Seidel, J.J.: Bounds for systems of lines and Jacobi polynomials. Philips Res. Rep. **30**, 91*–105* (1975)

[58] Derksen, H., Kemper, G.: Computational Invariant Theory. Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, Berlin (2002)

[59] Deutsch, D.: Uncertainty in quantum measurements. Phys. Rev. Lett. **50**, 631–633 (1983)

[60] Deza, M.M., Deza, E.: Encyclopedia of Distances, Springer-Verlag, Berlin (2013)

[61] Dimmock, J.O.: Representation theory for nonunitary groups. J. Math. Phys. **4**, 1307–1311 (1963)

[62] Dirac, P.A.M.: A new notation for quantum mechanics. Math. Proc. Cambridge **35**, 416–418 (1939)

[63] Eldar, Y.C., Forney, Jr., G.D.: Optimal tight frames and quantum measurement. IEEE Trans. Inf. Theory **48**, 599–610 (2002)

[64] Field, M.J.: Dynamics and Symmetry. Imperial College Press, London (2007)

[65] Flammia, S.T.: On SIC-POVMs in prime dimensions. J. Phys. A **39**, 13483–13493 (2006)

[66] Freed, D.S.: On Wigner's theorem. Geometry & Topology Monographs **18**, 83–89 (2012)

[67] Fritz, A., Hauser, H., Platonic stars. Math. Intelligencer **32**, 23–36 (2010)

[68] Fuchs, C.A.: *Quantum mechanics as quantum information (and only a little more).* In: Khrennikov, A.Yu. (ed.) Quantum Theory. Reconsideration of Foundations. Series Mathematical Modelling, 2, pp. 463–543. Växjö University Press, Växjö (2002)

[69] Fuchs, C.A., Jacobs, K.: Information-tradeoff relations for finite-strength quantum measurements. Phys. Rev. A **63**, 062305 (2001)

[70] Ghirardi, G.C., Marinatto, L., Romano, R.: An optimal entropic uncertainty relation in a two-dimensional Hilbert space. Phys. Lett. A **317**, 32–36 (2003)

[71] Giraud, O., Braun, P., Braun, D.: Quantifying quantumness and the quest for Queens of Quantum. New J. Phys. **12**, 063005 (2010)

[72] Gnutzmann, S., Życzkowski, K.: Rényi-Wehrl entropies as measures of localization in phase space. J. Phys. A **34**, 10123–10139 (2001)

[73] Grabowski, J., Kuś, M., Marmo, G.: Geometry of quantum systems: density states and entanglement. J. Phys. A **38**, 10217–10244 (2005)

[74] Grabowski, J., Kuś, M., Marmo, G.: Wigner's theorem and the geometry of extreme positive maps. J. Phys. A **42**, 345301 (2009)

[75] Grassl, M.: On SIC-POVMs and MUBs in dimension 6. Proceedings 2004 ERATO Conference on Quantum Information Science (Tokyo, September, 2004), pp. 60–61 (arXiv:0406175 [quant-ph])

[76] Grassl, M.: Tomography of quantum states in small dimensions. Electron. Notes Discrete Math. **20**, 151–164 (2005)

[77] Grassl, M.: Finding equiangular lines in complex space. MAGMA 2006 Conference (Technische Universität Berlin, July, 2006) *available online at* http://magma.maths.usyd.edu.au/Magma2006/

[78] Grassl, M.: Computing equiangular lines in complex space. Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth (Universität Karlsruhe, December, 2008) Lect. Notes Comput. Sci. **5393**, 89–104 (2008)

[79] Grey, R.M.: Entropy and Information Theory, 2nd ed. Springer, New York (2011)

[80] Haantjes, J.: Equilateral point-sets in elliptic two- and three-dimensional spaces. Nieuw Arch. Wisk. **22**, 355–362 (1948)

[81] Hall, M.J.W.: Quantum information and correlation bounds. Phys. Rev. A **55**, 100–113 (1997)

[82] Harremoës, P., Topsøe, F.: Inequalities between Entropy and Index of Coincidence derived from Information Diagrams. IEEE Trans. Inform. Theory **47**, 2944–2960 (2001)

[83] Havrda, J., Charvât, F.: Quantification method of classification processes. Concept of structural α-entropy. Kybernetika **3**, 30–35 (1967)

[84] Heinosaari, T., Mazzarella, L., Wolf, M.M.: Quantum tomography under prior information. Comm. Math. Phys. **318**, 355–374 (2013)

[85] Heinosaari, T., Ziman, M.: The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement. Cambridge UP, Cambridge (2011)

[86] Hoggar, S.G.: t-designs in projective spaces. European J. Combin. **3**, 233–254 (1982)

[87] Holevo, A.S.: Bounds for the quantity of information transmitted by a quantum communication channel. Probl. Inf. Transm. **9**, 177–183 (1973)

[88] Holevo, A.S.: Probabilistic and Statistical Aspects of Quantum Theory. North-Holland Publishing Company, Amsterdam (1982); Scuola Normale Superiore Pisa, Pisa (2011)

[89] Holevo, A.S.: Quantum systems, channels, information. A mathematical introduction. De Gruyter, Berlin (2012)

[90] Holevo, A.S.: Information capacity of a quantum observable. Probl. Inf. Transm. **48**, 1–10 (2012)

[91] Holevo, A.S.: Information capacities of quantum measurement channels. Phys. Scr. **T153**, 013034 (2013)

[92] Ivanović, I.D., Geometrical description of quantal state discrimination. J. Phys. A **14**, 3241–3245 (1981)

[93] Jarić, M.V., Michel, L., Sharp, R.T.: Zeros of covariant vector fields for the point groups: invariant formulation. J. Phys. (Paris) **45**, 1–27 (1984)

[94] Jones, K.R.W.: Quantum limits to information about states for finite dimensional Hilbert space. J. Phys. A **24**, 121–130 (1991)

[95] Jozsa, R., Koashi, M., Linden, N., Popescu, S., Presnell, S., Shepherd, D., Winter, A.: Entanglement cost of generalised measurements. Quantum Inf. Comput. **3**, 405–422 (2003)

[96] Jozsa, R., Robb, D., Wootters, W.K.: Lower bound for accessible information in quantum mechanics. Phys. Rev. A **49**, 668–677 (1994)

[97] Keller, K.J., Papadopoulos, N.A., Reyes-Lega, A.F.: On the realization of symmetries in quantum mechanics. Math. Semesterber. **55**, 149–160 (2008)

[98] Kendall, D.: Shape manifolds, procrustean metrics, and complex projective spaces. Bull. London Math. Soc. **16**, 81–121 (1984)

[99] Kimura, G.: The Bloch vector for N-level systems. Phys. Lett. A **314**, 339–349 (2003)

[100] Klyachko, A.: *Dynamical Symmetry Approach to Entanglement*. In: Gazeau, J.-P. et al. (eds.) Physics and Theoretical Computer Science. From Numbers and Languages to (Quantum) Cryptography, pp. 25–54. IOS Press, Amsterdam (2007)

[101] Krishna, M., Parthasarathy, K.R.: An entropic uncertainty principle for quantum measurements. Sankhyā **64**, 842–851 (2002)

[102] Kwapień, J., Słomczyński, W., Życzkowski, K.: Coherent states measurement entropy. J. Phys. A **30**, 3175–3200 (1997)

[103] Lang, M.D., Caves, C.M., Shaji, A.: Entropic measures of non-classical correlations. Int. J. Quantum Inform. **9**, 1553–1586 (2011)

[104] Lemmens, P.W.H., Seidel, J.J.: Equiangular lines. J. Algebra **24**, 494–512 (1973)

[105] Lieb, E.H.: Proof of Wehrl's entropy conjecture. Comm. Math. Phys. **62**, 35–40 (1978)

[106] Lieb, E.H., Solovej, J.P.: Proof of an entropy conjecture for Bloch coherent spin states and its generalizations. Acta Math. **212**, 379–398 (2014)

[107] Lim, C., Montaldi, J., Roberts, M.: Relative equilibria of point vortices on the sphere. Physica D **148**, 97–135 (2001)

[108] Maassen, H., Uffink, J.B.M.: Generalized entropic uncertainty relations. Phys. Rev. Lett. **60**, 1103–1106 (1988)

[109] Marshall, A.W., Olkin, I., Arnold, B.C.: Inequalities: Theory of Majorization and Its Applications. Springer, New York (2011)

[110] Massar, S.: Uncertainty relations for positive operator valued measures. Phys. Rev. A **76**, 042114 (2007)

[111] Memoli, F.: *Gromov-Hausdorff distances in Euclidean space*. In: Computer Vision and Pattern Recognition Workshops, 2008, CVPRW '08, pp. 1–8. IEEE Computer Society (2008)

[112] Michel, L.: Points critiques des fonctions invariantes sur une G-varieté. C. R. Acad. Sci. Paris **272**, 433–436 (1971)

[113] Michel, L.: Symmetry defects and broken symmetry. Configurations Hidden symmetry. Rev. Mod. Phys. **52**, 617–653 (1980)

[114] Michel, L., Zhilinskií, B.I.: Symmetry, invariants, topology, vol I. Basic tools. Phys. Rep. **341**, 11–84 (2001)

[115] Montgomery, D., Yang, C.: The existence of a slice. Ann. Math. **65**, 108–116 (1957)

[116] Naimark, M. A.: Spectral functions of a symmetric operator. Izv. Akad. Nauk. SSSR Ser. Mat. **4**, 277–318 (1940)

[117] Oreshkov, O., Calsamiglia, J., Muñoz-Tapia, R., Bagan, E.: Optimal signal states for quantum detectors. New J. Phys. **13**, 073032 (2011)

[118] Pauli, W.: Zur Quantenmechanik des magnetischen Elektrons. Zeit. f. Phys. **43**, 601–623 (1927)

[119] Pechukas, P.: Kolmogorov entropy and 'quantum chaos'. J. Phys. Chem. **86**, 2239–2243 (1982)

[120] Perelomov, A.M.: Generalized Coherent States and Their Applications. Springer, Berlin (1986)

[121] Price, R.: A Conversation with Claude Shannon: One Man's Approach to Problem Solving. IEEE Commun. Mag. **22**, 123–126 (1984)

[122] Prugovečki, E.: Information-theoretic aspects of quantum measurement. Int. J. Theor. Phys. **16**, 321–331 (1977)

[123] Quinn, C.M., Fowler, P., Redmond, D.: Computational Quantum Chemistry II - The Group Theory Calculator. Elsevier, Amsterdam (2005)

[124] Rastegin, A.E.: Comment on 'uncertainty relations for positive-operator-valued measures'. arXiv:0810.0038 [quant-ph]

[125] Rastegin, A.E.: Uncertainty relations for MUBs and SIC-POVMs in terms of generalized entropies. Eur. Phys. J. D **67**, 269 (2013)

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

[127] Rényi, A.: *On measures of entropy and information.* In: Proceedings of the Fourth Berkeley Symp. Math. Statist. Prob. 1960, Vol. I, pp. 547–561. University of California Press, Berkeley (1961)

[128] Robertson, S.A.: Polytopes and Symmetry. Cambridge UP, Cambridge (1984)

[129] Robertson, S.A., Carter, S.: On the Platonic and Archimedean solids. J. London Math. Soc. **2**, 125–132 (1970)

[130] Robertson, S.A., Carter, S., Morton, H.R.: Finite orthogonal symmetry. Topology **9**, 79–96 (1970)

[131] Rosado, J.I.: Representation of quantum states as points in a probability simplex associated to a SIC-POVM. Found. Phys. **41**, 1200–1213 (2011)

[132] Sánchez-Ruiz, J.: Improved bounds in the entropic uncertainty and certainty relations for complementary observables. Phys. Lett. A **201**, 125–131 (1995)

[133] Sartori, G., Valente, G.: Orbit spaces of reflection groups with 2, 3 and 4 basic polynomial invariants. J. Phys. A **29**, 193–223 (1996)

[134] Sartori, G., Valente, G.: Tools in the orbit space approach to the study of invariant functions: rational parametrization of strata. J. Phys. A **36**, 1913–1929 (2003)

[135] Sasaki, M., Barnett, S.M., Jozsa, R., Osaki, M., Hirota, O.: Accessible information and optimal strategies for real symmetrical quantum sources. Phys. Rev. A **59**, 3325–3335 (1999)

[136] Schroeck, Jr., F.E.: On the nonoccurrence of two paradoxes in the measurement scheme of stochastic mechanics. Found. Phys. **15**, 279–302 (1985)

[137] Schroeck, Jr., F.E.: On the entropic formulation of uncertainty for quantum measurements. J. Math. Phys. **30**, 2078–2082 (1989)

[138] Schroeck, Jr., F.E.: Quantum Mechanics on Phase Space. Kluwer, Dordrecht (1996)

[139] Scott, A.J.: Tight informationally complete quantum measurements. J. Phys. A **39**, 13507–13530 (2006)

[140] Scott, A.J., Grassl, M.: SICs: A new computer study. J. Math. Phys. **51** 042203 (2010)

[141] Senechal, M.: Finding the finite groups of symmetries of the sphere. Amer. Math. Monthly **97**, 329–335 (1990)

[142] Shannon, C.E.: A mathematical theory of communication. Bell Syst. Tech. J. **27**, 379–423 (1948)

[143] Shor, P.W.: Additivity of the classical capacity of entanglement-breaking quantum channels. J. Math. Phys. **43**, 4334–4340 (2002)

[144] Short, A.J., Wehner, S.: Entropy in general physical theories. New J. Phys. **12**, 033023 (2010)

[145] Słomczyński, W., Życzkowski, K.: Quantum chaos: an entropy approach. J. Math. Phys. **35**, 5674–5700 (1994); Erratum. J. Math. Phys. **36**, 5201 (1995)

[146] Słomczyński, W., Życzkowski, K.: Mean dynamical entropy of quantum maps on the sphere diverges in the semiclassical limit. Phys. Rev. Lett. **80**, 1880–1883 (1998)

[147] Słomczyński, W.: Dynamical Entropy, Markov Operators, and Iterated Function Systems. Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków (2003)

[148] Słomczyński, W., Szymusiak, A.: Highly symmetric POVMs and their informational power. arXiv:1402.0375 [quant-ph]

[149] Srinivas, M.D.: Quantum generalization of Kolmogorov entropy. J. Math. Phys. **19**, 1952–1961 (1978)

[150] Stoer, J., Bulirsch, R.: Introduction to numerical analysis. Springer, New York (2002)

[151] Suzuki, J., Assad, S.M., Englert, B.-G.: *Accessible information about quantum states: An open optimization problem.* In: Chen, G., Kauffman, L., Lomonaco, S.J. (eds.) Mathematics of Quantum Computation and Quantum Technology, pp. 309–348. Chapman & Hall/CRC, Boca Raton, FL (2007)

[152] Szymusiak, A.: Maximally informative ensembles for SIC-POVMs in dimension 3. arXiv:1405.0052 [quant-ph]

[153] Tribus, M.: *Information theory and thermodynamics.* In: Johnson, H., Boelter, L. (eds.) Heat Transfer, Thermodynamics and Education: Boelter Anniversary Volume, pp. 348–368. McGraw-Hill, New York (1964)

[154] Tsallis, C.: Possible generalization of Boltzmann-Gibbs statistics. J. Stat. Phys. **52**, 479–487 (1988)

[155] Uffink, J.B.M.: *Two New Kinds of Uncertainty Relations.* In: Proceeding of the Third international Workshop on Squeezed States and Uncertainty Relations, pp. 155–161. NASA Conference Publications 3270 (1994)

[156] Vale, R., Waldron, S.: Tight frames and their symmetries. Constr. Approx. **21**, 83–112 (2005)

[157] de Vicente, J.I., Sánchez-Ruiz, J.: Improved bounds in entropic uncertainty relations. Phys. Rev. A **77**, 042110 (2008)

[158] Waldron, S.: *Group Frames.* In: Casazza, P.G., Kutyniok, G. (eds.) Finite Frames. Theory and Applications, pp. 171–192. Birkhäuser, Basel (2013)

[159] Waldron, S.: Generalised Welch Bound Equality sequences are tight frames. IEEE Trans. Inform. Theory **49**, 2307–2309 (2003)

[160] Waterhouse, W.C.: Do symmetric problems have symmetric solutions? Amer. Math. Monthly **90**, 378–387 (1983)

[161] Wehner, S., Winter, A.: Entropic uncertainty relations – a survey. New J. Phys. **12**, 025009 (2010)

[162] Wehrl, A.: General properties of entropy. Rev. Mod. Phys. **50**, 221–260 (1978)

[163] Wigner, E.P.: Gruppentheorie und ihre Anwendung auf die Quantenmechanik der Atomspektrum. Fredrick Vieweg und Sohn, Braunschweig, Germany (1931), pp. 251–254; Eng. transl. *Group Theory and Its Application to the Quantum Theory of Atomic Spectra*, Academic Press Inc., New York (1959), pp. 233–236.

[164] Wilde, M.M.: Quantum Information Theory. Cambridge UP, Cambridge (2013)

[165] Xu, Z.F., Kawaguchi, Y., You, L., Ueda, M.: Symmetry classification of spin-orbit-coupled spinor Bose-Einstein condensates. Phys. Rev. A **86**, 033628 (2012)

[166] Yudin, V.A.: Minimum potential energy of a point system of charges (Russian). Diskret. Mat. **4**, 115–121 (1992); transl. in Discrete Math. Appl. **3**, 75–81 (1993)

[167] Zajtz, A.: Primitive geometric objects. Univ. Iagel. Acta Math. **11**, 105–111 (1966)

[168] Zauner, G.: *Quantendesigns.Grundzüge einer nichtkommutativen Designtheorie*, PhD thesis, Univ. Wien (1999); English translation *Quantum designs: Foundations of a noncommutative design theory*, Int. J. Quant. Inf. **9**, 445 (2011)

[169] Zefiro, L.: Vertex- and edge-truncation of the Platonic and Archimedean solids leading to vertex-transitive polyhedra. VisMath **13** (2011)

[170] Zefiro, L., Ardigò, M.R.: Description of the forms belonging to the 235 and $m3\bar{5}$ icosahedral point groups starting from the pairs of dual polyhedra: icosahedron-dodecahedron and Archimedean polyhedra-Catalan polyhedra. VisMath **9** (2007)

[171] Zhilinskií, B.I.: Symmetry, invariants, topology. II. Symmetry, invariants, and topology in molecular models. Phys. Rep. **341**, 85–171 (2001)

[172] Zhu, H.: SIC POVMs and Clifford groups in prime dimensions. J. Phys. A **43**, 305305 (2010)

[173] Zozor S., Bosyk, G.M., Portesi, M.: On a generalized entropic uncertainty relation in the case of the qubit. J. Phys. A **46**, 465301 (2013)

[174] Życzkowski, K.: Rényi extrapolation of Shannon entropy. Open Sys. & Information Dyn. **10**, 297–310 (2003)