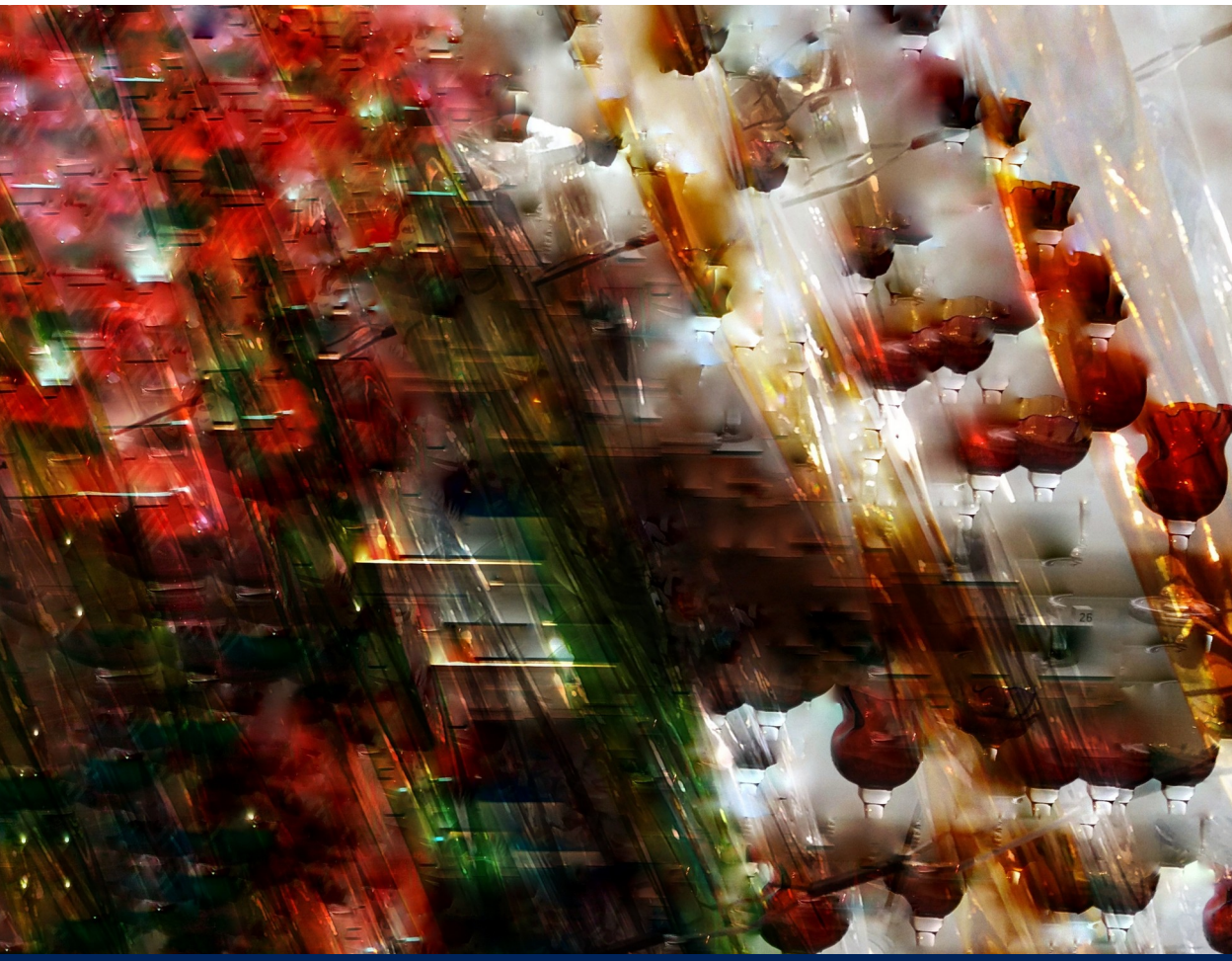
Stockholm University

Studies in the Geometry of Quantum Measurements

Irina Dumitru



Doctoral Thesis in Theoretical Physics at Stockholm University, Sweden 2020

Studies in the Geometry of Quantum Measurements

Irina Dumitru

Academic dissertation for the Degree of Doctor of Philosophy in Theoretical Physics at Stockholm University to be publicly defended on Thursday 10 September 2020 at 13.00 in sal C5:1007, AlbaNova universitetscentrum, Roslagstullsbacken 21, and digitally via video conference (Zoom). Public link will be made available at www.fysik.su.se in connection with the nailing of the thesis.

Abstract

Quantum information studies quantum systems from the perspective of information theory: how much information can be stored in them, how much the information can be compressed, how it can be transmitted. Symmetric informationally-Complete POVMs are measurements that are well-suited for reading out the information in a system; they can be used to reconstruct the state of a quantum system without ambiguity and with minimum redundancy. It is not known whether such measurements can be constructed for systems of any finite dimension. Here, dimension refers to the dimension of the Hilbert space where the state of the system belongs.

This thesis introduces the notion of alignment, a relation between a symmetric informationally-complete POVM in dimension d and one in dimension d(d-2), thus contributing towards the search for these measurements. Chapter 2 and the attached papers I and II also explore the geometric properties and symmetries of aligned symmetric informationally-complete POVMs.

Chapter 3 and the attached papers III and IV look at an application of symmetric informationally-complete POVMs, the so-called Elegant Bell inequality. We use this inequality for device-independent quantum certification, the task of characterizing quantum scenarios without modelling the devices involved in these scenarios. Bell inequalities are functions that are bound in classical theories more tightly than in quantum theories, and can thus be used to probe whether a system is quantum. We characterize all scenarios in which the Elegant Bell inequality reaches its maximum quantum value. In addition, we show that this inequality can be used for randomness certification.

Keywords: *quantum measurements, Bell nequalities, Weyl-Heiseberg group, device-independent certification, symmetric informationally-complete POVM.*

Stockholm 2020
http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-182527

ISBN 978-91-7911-218-9
ISBN 978-91-7911-219-6

Department of Physics

Stockholm University, 106 91 Stockholm

STUDIES IN THE GEOMETRY OF QUANTUM MEASUREMENTS

Irina Dumitru

Stockholm
University

Studies in the Geometry of Quantum Measurements

Irina Dumitru

ISBN print 978-91-7911-218-9
ISBN PDF 978-91-7911-219-6

Printed in Sweden by Universitetsservice US-AB, Stockholm 2020

Sammanfattning

Inom kvantinformation studeras kvantsystem från ett informationsteoretiskt perspektiv: hur mycket information kan lagras i systemet, hur mycket information som kan komprimeras i systemet och hur kan denna information överföras från ett system till ett annat?

Symmetriska, informationskompletta POVM: er är mätningar som är väl lämpade för att läsa informationen i ett givet kvantesystem; de kan användas för att rekonstruera ett tillstånd i ett kvantsystem utan tvetydighet och med minimal upprepning. Det finns inget bevis för huruvida sådana mätningar kan konstrueras för något ändligt dimensionssystem. Med dimension menas här dimensionen av Hilbert-rymden, där systemets tillstånd hör hemma.

I denna avhandling introduceras orienteringsbegreppet (upplinjerading), på engelska alignment, orientering är ett förhållande mellan två symmetriska informations - kompletta POVM'ar, en i dimension d och en i dimension d (d-2), arbetet i denna avhandling bidrar till sökandet efter dessa mätningar. I kapitel 2 och i artiklarna I och II undersökes också de geometriska egenskaperna och symmetrierna för orienterade (upplinjerad) symmetriska informations - kompletta POVM'ar.

I kapitel 3 och i artiklarna III och IV undersöks användningen av symmetriska information-kompletta POVM'ar, den *Elegant Bell inequality*. Vi använder denna ojämlikhet för en kvantcertifiering som är instrumentoberoende, uppgiften att karakterisera kvantmekaniska scenarier utan att modellera de instrumentar som är involverade i dessa scenarier. Bell ojämlikheter är funktioner som begränsas snävare i klassiska teorier än i kvantteorier, och kan således användas för att undersöka om ett system är kvantmekaniskt. Vi karakteriserar alla scenarier där *the Elegant Bell inequality* uppnår sitt maximala kvantvärde. Dessutom visar vi att denna ojämlikhet kan användas för att certifiera slumpmässighet.

List of Papers

The following papers, referred to in the text by their Roman numerals, are included in this thesis.

I **Dimension towers of SICs. I. Aligned SICs and embedded tight frames.** M. Appleby, I. Bengtsson, I. Dumitru, S. Flammia *Journal of Mathematical Physics* **58**, 112201 (2017).
DOI: 10.1063/1.4999844

II **Aligned SICs and embedded tight frames in even dimensions.** O. Andersson, I. Dumitru. *Journal of Physics A: Mathematical and Theoretical* **52(42)**, 425302 (2019).
DOI: 10.1088/1751-8121/ab434e

III **Self-testing properties of Gisin's elegant Bell inequality.** O. Andersson, P. Badziąg, I. Bengtsson, I. Dumitru, A. Cabello, *Physical Review A* **96(3)**, 032119 (2017).
DOI: 10.1103/PhysRevA.96.032119

IV **Device-independent certification of two bits of randomness from one entangled bit and Gisin's elegant Bell inequality** O. Andersson, P. Badziąg, I. Dumitru, A. Cabello, *Physical Review A* **97(1)**, 012314 (2018).
DOI: 10.1103/PhysRevA.97.012314

Author's contribution

Paper I I ran numerical calculations, checking for alignment in about half of the available cases, ruling out false leads, and establishing a numerical connection between alignment and geometric properties.

Paper II I contributed to refining the research question. I did calculations and co-wrote the paper.

Paper III I calculated implications of the maximal violation on the anticommutators and helped write the paper.

Paper IV I participated in blackboard discussions, where most of the calculations developed.

Contents

List of Figures

1. Introduction

The pure states of quantum systems are most often denoted by $|\Psi\rangle$, a notation that originates with Schrödinger, who used Ψ for the wave-function in his formulation of quantum mechanics. Currently, we most commonly think of pure states as rays in the projective Hilbert space. A ray is an equivalence class, containing vectors in the complex Hilbert space such that $|v\rangle = \lambda|u\rangle$, where λ is a complex number. The evolution of a system is represented as operators acting on the state. This is in the broadest terms the framework of the work in this thesis, and the Hilbert space is our playground.

Although questions about the geometry of the Hilbert space and its operators are of interest from a fundamental perspective in quantum mechanics, it is through the lens of quantum information theory that the particular research questions addressed in this thesis have developed.

Quantum information theory is concerned with looking at quantum systems from an information point of view, rather than a physical one. In this theory, quantum systems are understood to be characterized by the way information is stored in them. The evolution of systems is seen as information processing: copying, transmitting, deleting, introducing errors, correcting errors, reading, compressing etc. The notion of a *qubit*, analogous to the notion of a bit in classical information theory, is perhaps the simplest example that can offer an entry point to the methods and goals of quantum information theory.

A classical bit is an abstract unit of information that can take two values: 0 or 1. All information, in all contexts, can be thought of as being encoded in bits; and this way of thinking has become by now very common, with the rise of computers in the past 70 years. The physical support of bits can be dots on a paper (black and white corresponding to the values of 0 and 1), the state of a transistor, as in RAM memory, indentations on a metallic plate as in CDs, or columns of liquid as in military watches.

While the classical systems mentioned above are obviously very different physically, and implementing each of them comes with its own technology, from the point of view of classical information theory they

are equivalent. Information theory aims to answer questions such as how much information can be compressed, what the bound is on errors that can be tolerated in a system, how errors can be minimized or corrected, in a system-independent way. It also aims to design protocols for controlling and using information in a system-independent way, and then adapt their implementation to the physical systems.

Quantum information theory aims to do the same things, in the quantum realm. It was pioneered in the 70s and 80s, by Holevo, Kraus, Lindblad, Feynman and others (1). It represented a shift in the practice and goals of quantum physicists: not guided solely by trying to understand quantum systems, we now try to design and control them.

Quantum systems are physically different from classical ones, and this translates to a difference in how information is stored in them. While it is possible to represent quantum information in terms of classical information, this is very inefficient and in some sense unnatural. The qubit, the abstract unit of information in quantum systems, can take the values

$$\alpha|0\rangle + \beta|1\rangle,$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. The complex coefficients could of course be stored in classical bits. The introduction of additional qubits introduces *quantum entanglement*, making the system scale exponentially in terms of the number of classical bits needed and making it unfeasible to simulate quantum systems on classical ones.

The mathematical objects discussed in the first part of this thesis, the symmetric informationally -complete quantum measurements, arise naturally in quantum information theory, as they are measurements that are, in some sense, optimal for quantum tomography, the task of reading the information in a system (2). It is an open problem whether such measurements can be constructed for systems of any dimension. Here, the dimension of the system refers to the size of the Hilbert space where the state of the system is represented.

Chapter 2 covers this topic. First I introduce symmetric informationally - complete measurements, characterizing them both in quantum terms and in the terms of linear algebra. I then cover the necessary group theory, discussing the Weyl-Heisenberg group and the Clifford group. I finally present the results of the work I have been involved with on this topic. This work has started with the introduction of alignment, a relation between symmetric informationally - complete measurements in spaces of different dimensions. Alignment is based on numerical evidence from all known symmetric informationally-complete measurements, and

conjectured to hold in general. The attached papers I and II explore the implications of alignment on the geometric structure and symmetries of these measurements, and the results in these papers are summarised in Chapter 2. The most promising result is that alignment offers an intuition towards constructing symmetric informationally-complete measurements of high dimension starting from low dimensional measurements. Chapter 2 collects the results in Papers I and II in a self-contained way. However, I refer to the papers for the proofs.

The second part of my project deals with applications of symmetric informationally - complete measurements in Bell inequalities and device-independent quantum certification.

Bell inequalities are functions that are bound more tightly in classical theories than in quantum ones. Checking whether a system violates the classical bound of a Bell inequality is often used to probe whether a system is quantum. The maximal violation of Bell inequalities, i.e. the saturation of the quantum bound, is also a useful test; in particular it can be used to certify experimental set-ups.

Device-independent certification, the task of characterizing quantum systems without modelling the devices involved in creating or measuring these systems, is a powerful tool, unique to quantum information theory. Information theory is often concerned with adversarial scenarios, such as how to securely transfer information when there are malicious eavesdroppers around, or how to generate random numbers with a source that could have been pre-programmed by an untrustworthy manufacturer. The appeal of these scenarios comes from the fact that they are applied, but there are underlying theoretical considerations behind them. Developing protocols and tasks that are robust to interference is both a practical question for the nascent quantum information industry and a conceptually interesting question about the nature of quantum systems.

In chapter 3, I introduce Bell inequalities in detail, illustrate them with the aid of the most famous of them, the Clauser-Horne-Shimony-Holt Bell inequality, and then introduce a Bell inequality that uses symmetric informationally - complete measurements, called the elegant Bell inequality. The chapter then introduces two applications of quantum certification: self-testing and randomness certification. The attached papers II and IV are about using the elegant Bell inequality for these two applications, respectively, and chapter 3 summarises the results contained in these papers.

2. Symmetric Informationally-Complete POVMs

We encounter now the central objects in this thesis: symmetric informationally - complete POVMs, or SIC-POVMs. These represent a particular class of quantum measurements. POVM is an abbreviation of "positive operator valued measure", a rather confusing historical name for a generalized quantum measurement (or rather, for the mathematical counterparts of quantum measurements).

From a mathematical point of view, a generalized quantum measurement for a quantum system of dimension d consists of a set of d-dimensional positive operators $\{E_i\}$ resolving the identity: $\sum_i E_i = I$. The operators E_i are called effects or POVM elements associated with the measurement.

Below I follow the standard quantum information textbook by Nielsen and Chuang (1) to introduce generalized quantum measurements. Let a measurement described by measurement operators M_i be performed on a quantum system in state $|\Psi\rangle$. The probability of outcome i is $p(i) = \langle\Psi|M_i^\dagger M_i|\Psi\rangle$. We define

$$E_i = M_i^\dagger M_i. \tag{2.1}$$

Constructed this way, $\{E_i\}$ are guaranteed to have positive eigenvalues. From the fact that the probabilities $p(i)$ sum to one, it follows that the operators E_i must sum to the identity. The set of operators $\{E_i\}$ are sufficient to determine the probabilities of the different measurement outcomes. To reconstruct the state of the system from POVM measurements, we need to collect statistics, by repeating the measurements on an infinite number of copies of the system. In practice, of course, the number of copies used is always finite and limited, and our information about the state is thus subject to errors.

An informationally-complete POVM (or IC-POVM) is a special case of a POVM, one that can distinguish between any two quantum states, pure or mixed (3). The state of a d-dimensional system is given by a $d \times d$ density matrix, ρ. The matrix is characterized by $d^2 - 1$ real

parameters, one degree of freedom being eliminated by the condition $\mathrm{Tr}\rho = 1$. To reconstruct an arbitrary state we then need POVMs of at least d^2 elements proportional to one-dimensional projectors E_i, giving $d^2 - 1$ probabilities (the condition that the set $\{E_i\}$ resolves the identity reduces the number of linearly independent effects by 1). E_i being a projector means that there exists a state $|\Psi_i\rangle$ such that:

$$E_i = \frac{1}{d}|\Psi_i\rangle\langle\Psi_i| \tag{2.2}$$

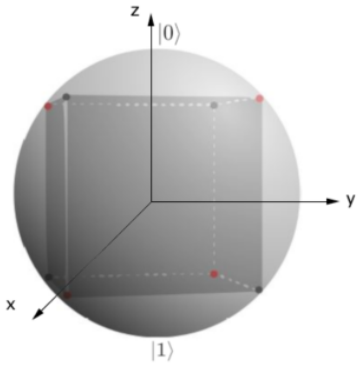


Figure 2.1: The Hilbert space of a qubit is the Bloch sphere, a two-dimensional space. A symmetric informationally-complete POVM consists of four effects proportional to projective measurements, having the same inner product two-by-two. Here we see illustrated two SIC-POVMs in dimension 2, one in black and one in red.

Symmetric informationally-complete POVMs are informationally complete POVMs obeying the additional condition:

$$d^2\mathrm{Tr}(M_i M_j) = |\langle\Psi_i|\Psi_j\rangle|^2 = \frac{1}{d+1} \tag{2.3}$$

for $\forall i \neq j$. That is to say, they have the same inner product two-by-two (see Figure 1).

Noting that a SIC-POVM can be then described by the d^2 vectors $|\Psi_i\rangle$, a geometric framework for dealing with SIC-POVMs becomes available. This framework will turn out to be the intuitive and natural one in many of the applications and problems we are concerned with, and from here on we will use the name SIC-POVM to refer to the set of d-dimensional vectors $\{|\Psi_i\rangle\}$ rather than to the set of projectors obtained from them.

From a geometric point of view, SIC-POVMs are a special case of equiangular tight frames, or, for short, ETFs. In this language, POVMs are called tight frames, and the symmetry condition is equivalent to equiangularity. An equiangular tight m-frame in a d-dimensional Hilbert space is a set of m unit-length vectors $|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{m-1}\rangle$ which satisfies the two conditions

$$\frac{d}{m}\sum_{i=0}^{m-1}|\psi_i\rangle\langle\psi_i| = 1 \tag{2.4}$$

$$|\langle\psi_i|\psi_j\rangle|^2 = \frac{m-d}{d(m-1)} \text{ if } i \neq j, \tag{2.5}$$

The first condition establishes tightness of the frame and is equivalent to the condition of resolving the identity for POVMs. The second condition establishes equiangularity, and thus symmetry of the corresponding POVM. Informational completeness is an additional condition that translates into fixing the number of vectors in the frame to $m = d^2$ and, implicitly, the value of the common angle between the vectors to

$$|\langle\psi_i|\psi_j\rangle|^2 = \frac{1}{d+1} \text{ if } i \neq j. \tag{2.6}$$

Such a frame must contain at least d vectors, as this is necessary in order to resolve the identity. It can be easily shown that the maximum number of vectors in such a frame is d^2, see (4). A minimal equiangular tight frame consists of d vectors and is the same as an orthonormal basis, or a von Neumann measurement. A maximal ETF correpsonds to a SIC-POVM. An ETF can be represented as d^2 equiangular vectors through the origin of the complex projective space C_d, each vector along the direction of the 1-dimensional space that it spans. From here on we drop the *POVM* from the name, and refer to the set $\{\Psi_i\}$ as simply a SIC.

Figure 1 illustrates a SIC in a two-dimensional Hilbert space, but it cannot be easily generalized to Hilbert spaces of arbitrary dimension. In fact, the problem of the existence of SIC-POVMs in Hilbert spaces of any finite dimension is an open problem. Zauner was among the first to signal the importance of these geometric structures in his doctoral thesis (5), which he approached from the perspective of *design theory*, which investigates combinatorial properties of finite sets. An equivalent characterization comes from this theory, where SICs correspond to tight complex projective 2-design. We will not delve into this frame-work, but a concise introduction to design theory can be found in Sec. 2 of (6).

In his thesis, Zauner also introduced the conjecture that in all finite dimensions at least one SIC exists that is covariant under the discrete Weyl-Heisenberg group. He further conjectured that at least one such SIC has an order 3 unitary symmetry. These conjectures have been guiding the search for SIC-POVMs ever since. As a result of extensive and careful numerical searches, we are now confident that in Hilbert spaces up to dimension 50 all Weyl-Heisenberg covariant SICs are known (7). Zauner conjectures have held so far. Interestingly, all of the known SICs have the symmetry conjectured by Zauner. Furthermore, at least one numerical SIC has been found in each dimension up to 193 (8), and there are several known SICs in higher dimensions, with the highest dimension being 2208 (8). Exact solutions are known in some dimensions, the highest being 323 (9).

In practice, the assumption of covariance under the Weyl-Heisenberg group has been used in most searches, and, as a result, almost all the known SICs are covariant under this group. The only known exception is in dimension 8, a SIC known as *the Hoggar lines*, which is covariant under the tensor product of lower-dimensional Weyl-Heisenberg groups (such a product is not necessarily a Weyl-Heisenberg group itself). In the attached papers we have restricted our study to WH-covariant SICs, and our results only apply to such SICs. Therefore, from here on, all SICs discussed are assumed to be covariant under the Weyl-Heisenberg group, or, equivalently, to form an orbit under this group. I will, however, use the notation WH-SIC for Weyl-Heisenberg covariant SICs in the context of mathematical proofs, for rigour. In the next section I will introduce the Weyl-Heisenberg group, then proceed with summarising our results, treating separately Hilbert spaces of even and odd dimension. [1] This means that knowing the group and one of the vectors in a given SIC one can obtain the other d^2-1 vectors by applying the group elements to the known vector. We can thus identify a SIC by such a vector alone, and indeed we will do so in most situations. This vector is called a fiducial; there exists a preferred choice of fiducial that makes the symmetries of the SIC look nicer, and this we call a *centered fiducial*. I will return to this issue, and provide a definition, in section 2.0.2.

[1] In prime dimensions it has been proven, by Zhu (10), that, if a SIC is covariant under any group, it must be covariant under the d-dimensional Weyl-Heisenberg group. No such proof exists for non-prime dimensions.

2.0.1 The discrete Weyl-Heisenberg group

The Weyl-Heisenberg group is an important presence in quantum mechanics. Weyl was among the first to try and formulate quantum mechanics in terms of group theory, in his 1928 book *The Theory of Groups and Quantum Mechanics* (11), where he makes the case that the major problems in quantum theory at the time, such as non-commuting physical quantities, can be tackled through the framework of groups. This idea, formulated explicitly in the first introduction of his volume, was not very popular among quantum physicists for a couple of decades; in fact, the occasional occurrence of groups in quantum mechanics was often referred to as "the group pest". But as other mathematical tools reached their limits in quantum mechanics (12), groups became popular in the '40s and '50s. Nowadays, group theory is seen as integral to the study of quantum systems, and students get introduced to it very early. There are of course the traditional examples of the rotation and Lorentz groups, as well as the permutation group; these had been accepted as useful tools even in the period of skepticism over groups in quantum mechanics. But the Weyl-Heisenberg group, together with Lie algebras, are accepted and taught as essential for the conceptual framework of quantum mechanics, rather than as tools that come from group theory.

The Weyl-Heisenberg group can be defined in Hilbert spaces of any dimension. The standard coherent states, often referred to as the most classical of quantum states, form an orbit under the Weyl-Heisenberg group in the infinite dimensional Hilbert space. That is, from any coherent state all others can be reached by applying the elements of the group, effectively providing a group-theoretical formulation of these states. Similarly, a SIC of the type we are interested in forms an orbit under the Weyl-Heisenberg group defined in a finite dimensional Hilbert space. The universality of the Weyl-Heisenberg group seems to promise some universality to the SIC problem.

One of Weyl's most treasured points in his book is that there is no conceptual difference between discrete and continuous groups, and no need to draw sharp mathematical distinctions between these two cases. However, in practice it remains simpler to handle continuous and discrete groups separately and, since it is only finite dimensional Hilbert spaces that we need for our study of SICs, I will restrict my treatment of the Weyl-Heisenberg group to the discrete case in this thesis (as this is what we need for finite dimensions).

The discrete Weyl-Heisenberg group has three generators: ω, X, Z. The definitional constraints are that the generators have order d,

ω commutes with all the group elements, and the other two generators satisfy the commutation relation $ZX = \omega XZ$. Weyl has proven that if we have an irreducible unitary representation of WH(d) on an d-dimensional Hilbert space, than the representation is unique up to a choice of basis, and ω is the identity operator multiplied by a d-th root of unity, usually chosen as $\omega = e^{2\pi i/d}$ (11, Ch. IV, §15). Uniqueness gives us the freedom to choose a basis where Z is diagonal, and we choose the basis in which X and Z are represented by generalized Pauli matrices:

$$X|\,k\,\rangle = |\,k+1\,\rangle \tag{2.7}$$

and

$$Z|\,k\,\rangle = \omega^k|\,k\,\rangle, \tag{2.8}$$

the addition being modulo d.

It is, for technical reasons, convenient to introduce $\tau = -\omega^{1/2}$ to replace ω whenever working with SICs. If d is odd, then τ is still a d-th root of unity, but if d is even, then τ is a $2d$-th root of unity, and thus we are effectively enlarging the group by adding τ. However, since τ commutes with all the elements of the group, we are only enlarging the center[1], and algebraic relations between the elements of the enlarged group remain the same. We will still call the enlarged group the Weyl-Heisenberg group; this is common practice (13).

The Weyl-Heisenberg group is the group generated by τ, X, and Z:

$$D_{i,j} = \tau^{ij} X^i Z^j. \tag{2.9}$$

We call the elements of the group "displacement operators", since their importance for our SIC problem is given by how they displace the fiducial vector. They satisfy

$$\mathrm{Tr}(D_{ij} D^\dagger_{i'j'}) = d\delta_{ii'}\delta_{jj'} \tag{2.10}$$

and consequently they form a unitary operator basis. By definition, this is a basis in the space of operators acting on the Hilbert space, such that each element of the basis is unitary. In quantum computation, these bases are called *nice error bases*, as they are used to discretize computational errors, enabling error-correction.

We introduce the notation $p = \binom{i}{j}$ in order to keep track of indices more easily. The displacement of the SIC fiducial $|\,\Psi_0\,\rangle$ by the Weyl-Heisenberg group can be written as:

$$|\,\Psi_p\,\rangle = D_p|\,\Psi_0\,\rangle. \tag{2.11}$$

[1]The center of a group is the set of all elements that commute with every element.

Since the Weyl-Heisenberg operators form an orthogonal basis, any operator acting on $\mathcal{H}^d$ admits a unique decomposition

$$A = \sum_p a_p D_{-p}, \quad a_p = \frac{1}{d} \mathrm{Tr} D_p A. \tag{2.12}$$

In particular, the projector corresponding to the SIC fiducial can be expressed as

$$|\Psi_0\rangle\langle\Psi_0| = \frac{1}{d} \sum_p D_{-p} \langle\Psi_0|D_p|\Psi_0\rangle. \tag{2.13}$$

This tells us immediately that any SIC can be reconstructed from the sets of overlaps of each component with the fiducial. We introduce the *overlap phases*:

$$e^{i\theta^{(d)}_{i,j}} = \begin{cases} 1 & \text{if } i = j = 0 \mod d, \\ \sqrt{d+1}\langle\, \psi_{0,0}\,|\,\psi_{i,j}\,\rangle & \text{otherwise.} \end{cases} \tag{2.14}$$

The upperscript (d) next to θ marks the dimension. Defining $e^{\theta^{(d)}_{0,0}}$ as 1 rather than $\sqrt{d+1}$ is a matter of convenience. Overlap phases play a major role in our approach of the SIC problem. They naturally introduce number theoretical considerations into the study of SIC, but we also use them in order to characterize SICs from a geometric point of view. The connection between these aspects is the most promising aspect of the work I have been involved in.

The commutation rule for the Weyl-Heisenberg group is

$$D_p D_q = \omega^{<p,q>} D_q D_p, \tag{2.15}$$

where the exponent of ω turns out to be the symplectic form, $< p, q >= p_1 q_2 - p_2 q_1$.

The composition rule of the group is

$$D_p D_q = \tau^{<p,q>} D_{q+p}. \tag{2.16}$$

The addition is modulo d. Here we again use τ. In fact, it is this composition rule that τ was introduced to simplify. In terms of ω, the left-hand side would look as: $\omega^{2^{-1}<p,q>}$. Raising to the power -1 is done modulo d, when d is odd. If d is even, the inverse does not exist, and the composition rule needs to be slightly modified, hence the introduction of τ (14). This is one of the more visible effects of the fact that odd and even cases are profoundly different, a difference which leads us to treat them separately.

2.0.2 The extended Clifford group and the symplectic group

The Weyl-Heisenberg group in any dimension is a subgroup of the group of unitaries in the same dimension. Its normalizer is the set of operators with respect to which it is a closed subgroup, i.e. operators that permute its elements:

$$UD_pU^\dagger = D_q = D_{f(p)}, \tag{2.17}$$

where $f(p)$ is a permutation. The normalizer is a group itself, and we call it the *Clifford group*.

To tackle the SIC problems I am interested in, we will need to enlarge the Clifford group by anti-unitaries that leave the Weyl-Heisenberg group unchanged. We call the group containing both unitaries and anti-unitaries the *extended Clifford group*, but we keep the notation U for the operators in the extended group. A detailed description of the extended Clifford group in relation to SICs can be found in (14).

Trivially, the operators in the extended Clifford group also permute the elements of each SIC, thus the Clifford group contains the stability group of the SIC.

It can be proven, see (14) that $f'(p)$ is linear in the elements of p: $f'(p) = Mp$, with M a 2×2 matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

A correspondence is thus established between the elements of the extended Clifford group and such 2×2 matrices, to each U corresponding a M.

To determine the form of such matrices M, we look at the Clifford operators acting on a product of Weyl-Heisenberg operators:

$$UD_pD_qU = U\tau^{<p,q>}D_{p+q}U^\dagger = \tau^{<p,q>}D_{M(p+q)} \tag{2.18}$$

where we used the composition rule in equation (2.15).

In the LHS of the above we can insert $I = UU^\dagger$:

$$UD_pD_qU^\dagger = UD_pU^\dagger UD_qU^\dagger = D_{Mp}D_{Mq} = \tau^{<Mp,Mq>}D_{Mp+Mq}, \tag{2.19}$$

From here on we can continue the discussion of even and odd dimensions together only by introducing $\bar{d}$, as:

$$\bar{d} = \begin{cases} d & \text{if } d \text{ is odd} \\ 2d & \text{if } d \text{ is even.} \end{cases} \tag{2.20}$$

What follows is valid for all dimensions, but note that $\bar{d}$ comes into some of the definitions (not all), and $\bar{d}$ is calculated differently in odd and even dimensions. From (2.18) and (2.19) it follows that only the matrices M preserving the relation $< p,q >=< Mp, Mq >$ modulo $\bar{d}$, i.e. matrices preserving the symplectic form of any pair (p,q), correspond to elements of the Clifford group.

The group of 2×2 matrices that correspond to the Clifford group is then the symplectic group $SL(2, \mathbb{Z}_{\bar{d}})$, that is, the set of 2×2 matrices with entries in the ring of integers modulo $\bar{d}$ and determinant 1.[1]

The rule taking us from a symplectic matrix M to a Clifford unitary U_M is given by Appleby (14). If

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{2.21}$$

is a symplectic matrix for which β is invertible modulo $\bar{d}$, then,

$$U_M = \frac{1}{\sqrt{d}} \sum_{u,v=0}^{d-1} \tau_d^{\beta^{-1}(\alpha v^2 - 2uv + \delta u^2)} |u\rangle\langle v|, \tag{2.22}$$

in the basis relative to which X_d and Z_d are represented by generalized Pauli matrices (2.7). Symplectic matrices with β invertible modulo $\bar{d}$ are called *prime*. For non-prime M one can always find prime symplectic matrices M_1 and M_2 such that $M = M_1 M_2$, see (14). We then define

$$U_M = U_{M_1} U_{M_2}. \tag{2.23}$$

Different prime decompositions of M give rise to operators U_M which may differ by a phase factor.

The most common way we use for decomposing a non-prime matrix is:

$$U_{M_1} = \begin{pmatrix} 0 & -1 \\ 1 & x \end{pmatrix} \qquad\qquad U_{M_2} = \begin{pmatrix} \gamma + x\alpha & \delta + x\beta \\ -\alpha & -\beta \end{pmatrix},$$

solving for x in each case. When d is prime $x = 0$ is a solution.

Remember that we have the freedom to choose our fiducial in each SIC. It turns out that we can make a convenient choice that simplifies

[1] In dimension 2 the symplectic group and the special linear group coincide, as they both preserve areas. In higher dimensions, the special linear group preserve volumes, while the symplectic group preserve symplectic areas. We use *symplectic* in dimension 2, since the symplectic form appears in the composition rule of the Weyl-Heisenberg group.

many of our calculations, namely we can choose the fiducial such that it is left invariant by a symplectic operator in the extended Clifford group, while the other elements of the SIC are permuted:

$$U_M|\,\Psi_0\,\rangle = |\,\Psi_0\,\rangle \tag{2.24}$$

$$U_M|\,\Psi_p\,\rangle = |\,\Psi_{f'(p)}\,\rangle, \quad \text{for } p \neq (0,1), \tag{2.25}$$

where $f'(p)$ is a permutation function. We call a fiducial that obeys the above condition a *centered fiducial*. It is the established practice in the SIC community to present results in terms of the centered fiducial (in a particular basis, which will be discussed below); in the available lists of numerical SICs, such as (7) and (15), it is the centered fiducials that you will find.

Zauner (5) conjectured that in every finite dimension, a SIC fiducial can be found that is left invariant by an order 3 unitary. In many dimensions, including all odd prime dimensions, all order 3 unitaries are equivalent, and we usually choose as a representative the symplectic unitary matrix corresponding to the $SL(2,\mathbb{Z}_{\bar{d}})$ matrix:

$$F_Z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}. \tag{2.26}$$

The relevant unitary, now known as the Zauner unitary, is:

$$\langle j|U_Z|i\rangle = \frac{e^{i\xi}}{\sqrt{d}}\tau^{ij+j^2}, \tag{2.27}$$

with $\xi = \frac{\pi(d-1)}{12}$. Its eigenvalues are $e^{2\pi ik/3}$, with $k \in \{0,1,2\}$. The dimension of the eigenspace corresponding to k is

$$dim Z_k = \left\lfloor \frac{d+3-2k}{3} \right\rfloor, \tag{2.28}$$

where the brackets signify the *floor function*, returning the integer part of the argument.

This conjecture seems to hold. In practice, in every dimension where SIC fiducials have been found, at least one of them is stabilized by this matrix. In fact, almost all known fiducials are. However, in dimensions of the form $d = 9k+3$ and $d = 9k+6$, there exist inequivalent classes of order 3 matrices. In these dimensions there also exist at least one solution that is stabilized by the class represented by the Zauner unitary. But in dimensions $d = 9k+3$ there exist solutions that are stabilized by another order-3 unitary:

$$F_a = \begin{pmatrix} 1 & 3 \\ 3k & -2 \end{pmatrix}. \tag{2.29}$$

Up to dimension 48, the fiducials with these symmetries are 12b, 21e, 30d, 39g, 39h, 39i, 39j, 48e, 48g.

Many SICs have additional symmetries. Scott and Grassl (7) deduce two more general symmetries present in known solutions:

- in dimensions $N = k^2 - 1 = (k+1)(k-1) = 8$, 15, 24, 35, $48g$, ..., some fiducials have the additional order-2 symmetry U_{F_b}, corresponding to the symplectic:

$$F_b = \begin{pmatrix} -k & N \\ N & N-k \end{pmatrix}. \tag{2.30}$$

  The fiducials with this symmetry known to Scott and Grassl at the time are 8b, 15d, 24c, 35i, 35j, 48f. Dimensions of the form $k^2 - 1$ can be written as $N = d(d-2)$, for $d = k-1$. The fiducials with the additional symmetry U_{F_b} are of interest from a geometric point of view, as we will see in the next section, and in the accompanying papers I and II.

- in dimensions $N = (3k \pm 1)^2 + 3 = 4$, 7, 19, 28, 52, ..., some fiducials have the additional anti-unitary symmetry

$$F_c = \begin{pmatrix} \kappa & N - 2\kappa \\ N0 + 2\kappa & N - \kappa \end{pmatrix}, \quad \kappa = 3k^2 \pm k + 1 \tag{2.31}$$

Here is a good place to introduce an additional notation for SICs:

11c
3

Table 2.1: A SIC in dimension 11. The letter c distinguishes it from other SICs in the same dimension, labelling the extended Clifford orbit to which the SIC belongs. The alphabetical order carries no meaning, it mostly reflects the order in which the SICs were found. The number below is the order of the symmetry of the SIC, in this case 3.

Representing a SIC by a box, like above, comes in handy when trying to arrange SICs with similar properties in tables. Our main results are summarised in the next section in tables of this kind.

2.1 Results

In this section I will give an overview of the results of the work I have participated in on the topic of SICs. Most of the results presented here have been published, as the attached papers I and II. The last section of this chapter includes unpublished results. The main contribution of papers I and II taken together is the observation that a number theoretic relation between SICs in dimension d and SICs in dimension $d(d-2)$, called *alignment*, extends to the geometry of the SICs, and proof that this relation has implications on the geometry of the higher dimensional SIC, for all d.

Remember that the ultimate goal in SIC research is to obtain a proof of the existence of SICs in all finite dimensions, and, perhaps, a recipe for analytically calculating at least one SIC in an arbitrary dimension. The attached papers on SICs are working towards this goal in a modest way by helping point towards possible infinite ladders of SICs.

We observed that specific SICs in dimension d and SICs in dimension $d(d-2)$ are in a relation which we will call *alignment*.

Let us remember the overlap phases in dimension d:

$$e^{i\theta_{i,j}^{(d)}} = \begin{cases} 1 & \text{if } i=j=0 \mod d, \\ \sqrt{d+1}\langle\,\psi_{0,0}\,|\,\psi_{i,j}\,\rangle & \text{otherwise.} \end{cases} \tag{2.32}$$

We denote the corresponding phases in dimension $N=d(d-2)$ by $e^{i\theta_{i,j}^{(N)}}$.

Here number theoretical considerations come into play. For all known examples, these phase factors are always algebraic units in an abelian extension of the real quadratic field $\mathbb{Q}(\sqrt{D})$, where D is the square free part of $(d+1)(d-3)$ (16). The square free part of an integer $D=a\sqrt{b}$ is b, or, in other words, the product of the prime factors with multiplicity one. For example, for $d=4$, we get $(d+1)(d-3)=5*1=5$ and the square-free part is 5. For $d=5$, we have $(d+1)(d-3)=6*2=12=2^2*3$ and the square-free part is 3.

The value of D does not change when we substitute $d(d-2)$ for d:

$$(d(d-2)+1)(d(d-2)-3) = (d-1)^2(d+1)(d-3). \tag{2.33}$$

This is important, as it means that the field relevant in dimension d reappears as a subfield of the field relevant in dimension $N=d(d-2)$ (17).

We were motivated to look for a consistent relation between phases in these dimensions by an observation made by Gary McConnell, who

had been motivated to compare overlap phases in dimensions d and $d(d-2)$ by the relation between the fields mentioned above. McConnell noticed in a few specific cases that a subset of overlap phases appearing in dimension $N = d(d-2)$ are equal to the squares of overlap phases in dimension d (18). Our formal definition is that a WH-SIC in dimensions $N = d(d-2)$ is aligned with a WH-SIC in dimension d if, for some choice of fiducials in each SIC, if $i \neq 0 \bmod (d-2)$ or $j \neq 0 \bmod (d-2)$, then

$$e^{i\theta^{(N)}_{di,dj}} = \begin{cases} 1 & \text{if } d \text{ is odd,} \\ -(-1)^{(i+1)(j+1)} & \text{if } d \text{ is even,} \end{cases} \tag{2.34}$$

and if $i \neq 0 \bmod d$ or $j \neq 0 \bmod d$, then

$$e^{i\theta^{(N)}_{(d-2)i,(d-2)j}} = \begin{cases} -e^{2i\theta^{(d)}_{\alpha i+\beta j,\gamma i+\delta j}} & \text{if } d \text{ is odd,} \\ (-1)^{(i+1)(j+1)} e^{2i\theta^{(d)}_{\alpha i+\beta j,\gamma i+\delta j}} & \text{if } d \text{ is even,} \end{cases} \tag{2.35}$$

where α, β, γ, and δ are integers modulo d such that $\alpha\delta - \beta\gamma = \pm 1$. Whether one of the conditions 2.34 and 2.35 follows from the other is an open question, whose solution would have profound implications on the geometry of WH-SICs. No SIC is known which satisfies one of the conditions but not the other.

We checked and confirmed the presence of alignment between all candidate pairs of SICs available at the time. For example, the SIC labeled $6a$ (in dimension 6) and the SIC labeled $24c$ (in dimension $24 = 6 * 4$) are aligned. All pairs for which alignment has been checked numerically can be found in the following tables.

24c	35i	35j	63b	63c	80i	99b	99c	99d
6a	7a	7b	9a	9b	10a	11c	11a	11b

120b	120c	143a	143b	168a	323b	323c
12a	12b	13a	13b	14b	19d	19e

Table 2.1: Two-step ladders of aligned SICs

48g	48f	195d	195b	195a	195c
8b	8a	15d	15b	15a	15c
4a		5a			

Table 2.2: Three-step ladders of aligned SICs

The entries in Table 2.1 should be read as, for example, *SIC 24c is aligned to SIC 6a*, or, equivalently *SIC 24c and SIC 6a are in an alignment relation.* In Table 2.2 we have the cases for which it was possible to check d, $N = d(d-2)$, and $N' = N(N-2)$. For example, 48g is aligned to 8b which, in its turn, is aligned to 4a.

The numeric testing was exhaustive in that for all known SICs where potentially aligned SICs in the corresponding dimension $N = d(d-2)$ were known at the time, alignment is indeed present. For some SICs, for example 17a, no candidate for alignment (a SIC in dimension $255 = 17 * 15$) was known at the time we did this work, so we were not able to perform the check. In dimension 11 three SICs exist. In the corresponding dimension $99 = 11 * 9$ four different SICs are known, labeled a to d, and three of them are aligned to the 11-dimensional ones. In dimension 4, only one SIC is known, and $8b$ is aligned with it; both SICs in dimension 8 have SICs in dimension 48 aligned to them.

As new SICs have become available during my time on this project, we have tested them and found them to fit in the table. When we started, no SIC was available in dimension $195 = 15 * 13$ and so none of the four SICs in dimension 15 could be tested for alignment with a higher dimensional SIC . Later on, one 195-dimensional SIC became available through the work of Andrew Scott (15), and we immediately found it to be aligned with one of the 15-dimensional SICs. This is where our first conjecture comes into play.

Conjecture 1 *Any SIC in dimension d has a $d(d-2)$-dimensional SIC aligned to it.*

Believing in the conjecture, we expected at least three more SICs to exist in dimension 195, aligned with the remaining three 15-dimensional SICs, and we asked Scott to look for them. He did indeed find three SICs (19), and they turned out to be aligned to the ones we had in dimension 15. As it is clear from the tables above, the converse does not hold: SICs in dimensions $N = d(d-2)$ do not necessarily have a d-dimensional SIC to which they are aligned.

The above conjecture points towards infinity. If it can be proven, then the existence of an infinite number of SICs is proven. Not quite *any* finite dimension, but any dimension that can be decomposed into a product of two integer factors, the second being the first minus two.

As mentioned before, the difference between even and odd dimensions is very deep, and it concerns the behaviour of Weyl-Heisenberg groups under the tensor product, as well as the behaviour of parity

operators (in their turn connected to discrete Wigner functions (20)). Thus, the odd-dimensional spaces and even-dimensional spaces have been treated separately, in paper *I* and *II* respectively. Our results are formulated in the papers separately for the even and odd case. But the fundamental results can be captured in a parity-independent way, and they are formulated in this way here. The first result is Conjecture 1 as formulated above. The second is the implication of alignment to the geometry of the SICs:

Theorem 1 *Any aligned SIC in dimension $N = d(d-2)$ can be decomposed into $(d-2)^2$ equiangular tight d^2-frames, and, alternatively, into d^2 equiangular tight $(d-2)^2$-frames.*

We also had, at the time when we were looking for solutions in dimension 195, a conjecture about the order of a symmetry that aligned SICs would have. The newly found SICs in dimension 195 confirmed that as well. In the meantime, we have proven this particular conjecture. While the proof is different for odd and even dimensions, the following formulation captures the implication of alignment on symmetry in a parity-independent way:

Theorem 2 *Aligned SICs have symmetries of order double the order of the symmetry of the lower-dimensional SIC to which they are aligned.*

In the following sections, we go over the proofs of these results in odd and even dimensions separately. In a final section of this chapter, we present a simple expression of an exact SIC in dimension 35; this result has not been published. The inspiration for looking at the exact solution in dimension 35 came from the work of Appleby and Bengtsson in (21), where they look at some exact SICs in dimensions 5, 15, and 195, i.e. the ladder of dimensions that starts from 5. Looking at the ladder starting from 7 was a natural next step and, though the expression we find in dimension 35 is not as neat as the ones in dimension 15 and 195, it is still simpler than the expressions already known in the literature and, as such, it is useful for researchers in SICs to have access to it.

2.1.1 Odd dimensions

D. Gross came up with the idea of applying the ancient Chinese Remainder Theorem to the Weyl-Heisenberg group. This is possible in dimensions $n_1 n_2$ with n_1 and n_2 relatively prime. Gross called the application "Chinese remaindering" (22), and I will be using this term.

The presentation below is inspired by notes shared with me by Marcus Appleby (23).

In modern language, the Chinese Remainder Theorem states that the rings $\mathbb{Z}_{n_1 n_2}$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ are isomorphic, for n_1 and n_2 relatively prime. The details require a little care. The isomorphism that we rely on is explicitly given by

$$u \bmod n_1 n_2 \to (u \bmod n_1, u \bmod n_2). \tag{2.36}$$

For simplicity, we will write u for $u \bmod m$, u_1 for $u \bmod n_1$, and u_2 for $u \bmod n_2$.

A basis of the Hilbert space of dimension $n_1 n_2$, $\mathcal{H}^{n_1 n_2}$, is labelled by the elements in $\mathbb{Z}_{n_1 n_2}$, the ring of integers modulo $n_1 n_2$. Similarly, bases in the Hilbert spaces $\mathcal{H}^{n_1}$ and $\mathcal{H}^{n_2}$ are labeled by the elements of $\mathbb{Z}_{n_1}$ and $\mathbb{Z}_{n_2}$ respectively. $\mathbb{Z}_{n_j}$ is the ring of integers modulo n_j. The isometry between the rings then carries over to the Hilbert spaces, through the assignment $|u\rangle \to |u_1\rangle \otimes |u_2\rangle$. Thus, there exist an isometry from the Hilbert space of dimension $n_1 n_2$, $\mathcal{H}_{n_1 n_2}$, onto the tensor product of the Hilbert space in dimension n_1 and the Hilbert space in dimension n_2, $\mathcal{H}_{n_1} \otimes \mathcal{H}_{n_2}$.

We introduce here, for each subspace ($j = 1, 2$):

$$\bar{n}_j = \begin{cases} n_j & \text{if } n_j \text{ is odd,} \\ 2n_j & \text{if } n_j \text{ is even.} \end{cases} \tag{2.37}$$

In dimensions of the form $d(d-2)$ with d odd, we identify n_1 to d and n_2 to $d-2$. As d and $d-2$ are also odd, they are relatively prime. Chinese Remaindering then allows us to split the Hilbert space into a tensor product.

The Weyl-Heisenberg group then splits into the tensor product of the Weyl-Heisenberg group in dimension d and the Weyl-Heisenberg group in dimension $d-2$:

$$D^{d(d-2)}_{i,j} = D^{d}_{i,\kappa_2 j} \otimes D^{d-2}_{\kappa_1 i, j}. \tag{2.38}$$

In each subspace we face the same complication that lead us to introduce $\bar{d}$ in equation 2.20, that is, the symplectic form needed for the composition rule of the Weyl-Heisenberg group is taken differently in odd dimensions compared to even dimensions.

The integers κ_1 and κ_2 are the multiplicative inverses of n_1 and n_2 in arithmetic modulo $\bar{n}_2$ and $\bar{n}_1$, respectively. That is, $\kappa_1 n_1 = 1 \bmod \bar{n}_2$ and $\kappa_2 n_2 = 1 \bmod \bar{n}_1$.

To verify (2.38), we calculate the action of the left-hand side operator on $|\,u\,\rangle$ and the action of the right-hand side operators on $|\,u_1\,\rangle$ and $|\,u_2\,\rangle$:

$$D^{(n_1n_2)}_{i,j}|\,u\,\rangle = \tau^{ij}_{n_1n_2}\omega^{uj}_{n_1n_2}|\,u+i\,\rangle, \tag{2.39}$$

$$D^{(n_1)}_{a,\kappa_2 j}|\,u_1\,\rangle = \tau^{ij\kappa_2}_{n_1}\omega^{u_1\kappa_2 j}_{n_1}|\,u_1+i_1\,\rangle, \tag{2.40}$$

$$D^{(n_2)}_{i,j\kappa_1}|\,u_2\,\rangle = \tau^{ij\kappa_1}_{n_2}\omega^{u_2 j\kappa_1}_{n_2}|\,u_2+i_2\,\rangle. \tag{2.41}$$

We have $|\,u+i\,\rangle = |\,(u+i) \bmod n_1\,\rangle \otimes |\,(u+i) \bmod n_2\,\rangle$, and from that $|\,u+i\,\rangle = |\,u_1+i_1\,\rangle \otimes |\,u_2+i_2\,\rangle$. Equation (2.39) then becomes:

$$D^{(n_1n_2)}_{i,j}|\,u\,\rangle = \tau^{ij}_{n_1n_2}\omega^{uj}_{n_1n_2}(|\,u_1+i_1\,\rangle + |\,u_2+i_2\,\rangle). \tag{2.42}$$

We can, using

$$\tau_{n_1n_2} = \tau^{\kappa_2}_{n_1}\tau^{\kappa_1}_{n_2}, \tag{2.43}$$

$$\omega^{u}_{n_1n_2} = \omega^{u_1\kappa_2}_{n_1}\omega^{u_2\kappa_1}_{n_2}, \tag{2.44}$$

identify the coefficients, thus verifying (2.38).

2.1.2 Even dimensions

In even dimensions of the form $n = d(d-2)$, Chinese Remaindering is not immediately available. This is due to the fact that when n is even, d and $(d-2)$ also have to be even. Nevertheless, there is a tensor product structure hidden in even dimensional spaces as well, and we uncovered it, using a particular representation of the Weyl-Heisenberg group, together with the decomposition of the Hilbert space into a direct sum of spaces.

We take a factor of 2 out of each factor by introducing $n_1 = d/2$ and $n_2 = (d-2)/2$. The integers n_1 and n_2 are relatively prime, being consecutive integers. We have shown that the Hilbert space can be decomposed into a direct sum of four (n_1n_2)-dimensional subspaces,

$$\mathcal{H}^{(n)} = \bigoplus_{i,j=0}^{3} \mathcal{H}^{n_1n_2} \tag{2.45}$$

, and that the Weyl-Heisenberg group admits a representation such that the displacement operators with even indices are block-diagonal:

$$D_{2i,2j}^{(4n_{n2})} = (-1)^{ij} \begin{pmatrix} D_{i,j}^{(n_1 n_2)} & & & \\ & \omega_{2n_1n_2}^{i} D_{i,j}^{(n_1 n_2)} & & \\ & & \omega_{2n_1n_2}^{j} D_{i,j}^{(n_1 n_2)} & \\ & & & \omega_{2n_1n_2}^{i+j} D_{i,j}^{(n_1 n_2)} \end{pmatrix}. \tag{2.46}$$

We go on to apply Chinese Remaindering in each subspace of dimension $n_1 n_2$. The subspace displacement operators then split according to the Chinese Remainder Theorem, as described above in section 2.1.1:

$$D_{i,j}^{(n_1 n_2)} = D_{i,\kappa_2 j}^{(n_1)} \otimes D_{i,\kappa_1 j}^{(n_2)}. \tag{2.47}$$

The integers κ_1 and κ_2 are the multiplicative inverses of n_1 and n_2 modulo $\bar{n}_2$ and $\bar{n}_1$, respectively. We then prove that the displacement operators involved in equations 2.52 and 2.53 split into tensor products:

$$D_{di,dj}^{(n)} = \mathbb{1}_{n_1} \otimes \begin{pmatrix} D_{i,j}^{(n_2)} & & & \\ & \omega_{2n_2}^{i} D_{i,j}^{(n_2)} & & \\ & & \omega_{2n_2}^{j} D_{i,j}^{(n_2)} & \\ & & & \omega_{2n_2}^{i+j} D_{i,j}^{(n_2)} \end{pmatrix} \tag{2.48}$$

and

$$D_{(d-2)i,(d-2)j}^{(n)} = \begin{pmatrix} D_{-i,j}^{(n_1)} & & & \\ & \omega_{2n_1}^{i} D_{-i,j}^{(n_1)} & & \\ & & \omega_{2n_1}^{b} D_{-i,j}^{(n_1)} & \\ & & & \omega_{2n_1}^{i+j} D_{-i,j}^{(n_1)} \end{pmatrix} \otimes \mathbb{1}_{n_2}. \tag{2.49}$$

The proof of the above, presented in Paper II, follows from the availability in dimensions of the form $n = 4m$ of a particular representation of the Weyl-Heisenberg group, inspired by (24). In our case, $m = n_1 n_2$. In this representation, the generators X_N and Z_N are 4x4 block matrices, with mxm blocks:

$$X_N = \begin{pmatrix} 0 & 0 & X_m & 0 \\ 0 & 0 & 0 & \omega_{2m} X_m \\ \mathbb{1}_m & 0 & 0 & 0 \\ 0 & \mathbb{1}_m & 0 & 0 \end{pmatrix}, \quad Z_N = \begin{pmatrix} 0 & \mathbb{1}_m & 0 & 0 \\ Z_m & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega_{4m} \mathbb{1}_m \\ 0 & 0 & \omega_{4m} Z_m & 0 \end{pmatrix}, \tag{2.50}$$

where ω_{2m} is the $2m$-th root of unity, ω_{4m} is the $4m$-th root of unity, X_m and Z_m are the generalized Pauli matrices in dimension m, in the standard representation, and $\mathbb{1}_m$ is the identity matrix in dimension m:

$$\mathbb{1}_m = \sum_{u=0}^{m-1} |u\rangle\langle u|, \quad X_m = \sum_{u=0}^{m-1} |u+1\rangle\langle u| \quad Z_m = \sum_{u=0}^{m-1} \omega_m^u |u\rangle\langle u|, \quad (2.51)$$

The representation 2.50 acts on the total space $\mathcal{H}^{(n)}$.

2.1.3 Embedded equiangular tight frames

In both even and odd dimensions, the proof of Theorem 1 is equivalent to proving that the operators

$$\Pi_1 = \frac{d-1}{2d} \sum_{i,j=0}^{d-1} |\psi_{(d-2)i,(d-2)j}\rangle\langle\psi_{(d-2)i,(d-2)j}|, \quad (2.52)$$

$$\Pi_2 = \frac{d-1}{2(d-2)} \sum_{i,j=0}^{d-3} |\psi_{di,dj}\rangle\langle\psi_{di,dj}|, \quad (2.53)$$

formed by adding together specific subsets of the operators in a SIC, are projectors. If and only if the above operators are projectors, then the sets of vectors that go into them,

$$\{|\,\Psi_{di,dj}\,\rangle : i,j = 0 \ldots d-3\} \quad (2.54)$$

and

$$\{|\,\Psi_{(d-2)i,(d-2)j}\,\rangle : i,j = 0 \ldots d-1\}, \quad (2.55)$$

form an equiangular tight frame each, consisting of $(d-2)^2$ vectors and d^2 vectors respectively. (2.54) spans a $(d-1)(d-2)/2$-dimensional space, while (2.55) spans a $d(d-1)/2$-dimensional space. By shifting (2.54) using Weyl-Heisenberg displacement operators of the form $D_{(d-2)i,(d-2)j}$, we can effectively partition the SIC into d^2 equiangular tight $(d-2)^2$-frames. Similarly, by shifting (2.55) by $D_{di,dj}$, we partition the SIC into $(d-2)^2$ equiangular tight d^2-frames.

Detailed proofs for the odd and even case are provided in Paper I and II, respectively. Ostrovskyi and Yakymenko have independently arrived at the representation described in section 2.1.2, for even dimensions, in their 2019 paper (25).

2.1.4 Symmetries of aligned SICs

As stated in Theorem 2, we have found that aligned SICs have a total symmetry of order double the order of the symmetry of the lower dimensional SIC to which they are aligned. Theorem 2 is proven in Papers I and II, for the odd case and the even case respectively. In both cases, aligned SICs "inherit" the symmetries of the lower dimensional SIC to which they are aligned, and have an additional order 2 symplectic unitary symmetry. By the symmetries being inherited we mean that if the d SIC has as a symmetry the unitary or anti-unitary operator $U_M^{(d)}$, a d-dimensional operator corresponding to the symplectic matrix M by 2.22, then the $d(d-2)$-dimensional SIC has as a symmetry the operator $U_M^{(d(d-2))}$, which is also obtained from M by 2.22. The additional symmetry that we discovered fixes the fiducial (chosen such that the alignment conditions (2.34) and 2.35 are satisfied, which in all cases coincides with it being a centered fiducial) and permutes the other SIC elements.

The additional symmetry, in both odd and even dimensions, involves the parity operator on the Hilbert space. I will introduce parity operators here, highlighting the differences between odd and even dimensions, before proceeding on to the symmetry.

The most intuitive way to think of parity operators is as reflections through a plane or through a point. Indeed, the phrase first invokes the parity operators in particle physics or in solid state physics: operators that change the sign of the spatial coordinates of a state.

Mathematically, parity operators are involutions, i.e. operators that have $+1$ and -1 as eigenvalues and thus square to the identity operator. For our problem, the relevant of parity operators is that they reflect the indices of the displacement operators:

$$P^{(n)} D^n_{i,j} P^{(n)} = D^n_{-i,-j} \tag{2.56}$$

When n is odd, the index arithmetic is done modulo n, and the parity operator is periodic.

As $P^{(n)}$ belongs to the Clifford group, it can, according to (14), be written as $P^{(n)} = e^{i\phi} D^{(n)}_{i,j} U_M$, where $e^{i\phi}$ is a phase and U_M is a representation of the symplectic matrix M, as defined in 2.22.

In both odd and even dimensions, an option for M is:

$$M = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{2.57}$$

If we displace 2.56 by $D_{i,j}$, we get

$$D_{i,j}^{(n)} P^{(n)} D_{i,j}^{(n)} P^{(n)} = \mathbb{1}, \tag{2.58}$$

Let us apply the displaced parity operator to $D_{-i,-j}$:

$$D_{i,j} P D_{-i,-j} = D_{i,j} P D_{-i,-j} P P = D_{i,j} D_{i,j} P = D_{2i,2j} P, \tag{2.59}$$

where we have dropped the dimension in the notation of each operator. This means that $D_{2i,2j}P = PD_{-2i,-2j}$, and thus $P_{i,j} = D_{i,j}PD_{-i,-j}$ is also an order-2 operator and thus a parity operator, in the mathematical sense. We call these operators displaced parity operators.

If n is odd, then we can find some indices k, l such that $2i = k \bmod n$ and $2j = l \bmod n$, and thus we can write $D_{i,j}PD_{-i,-j} = D_{k,l}P$. All displaced parity operators then are conjugate to P and thus have the same spectrum, $(d+1)/2, (d-1)/2)$.

If n is even, in order to have $2i = k \bmod n$ and $2j = l \bmod n$, then k and l must be even too. We end up with two sets of displaced parity operators, characterized by different spectra depending on the parities of i and j:

$$\mathrm{Sp} P_{i,j}^{(n)} = \left(\frac{n+1-(-1)^{(i+1)(j+1)}}{2}, \frac{n-1+(-1)^{(i+1)(j+1)}}{2} \right) \tag{2.60}$$

In Paper I, we prove that for aligned SICs in dimensions of the form $n = d(d-2)$, where d is odd, this symmetry has the form:

$$U_b = \mathbb{1}_d \otimes P^{(d-2)}, \tag{2.61}$$

where $P^{(d-2)}$ is the parity operator in dimension $d-2$.

In paper II, we prove that for aligned WH-SICs in dimensions of the form $n = d(d-2)$, where d is even, the symmetry has the form:

$$U_b = \begin{pmatrix} \mathbb{1}_{n_1} \otimes P_{0,0}^{(n_2)} & & & \\ & -\mathbb{1}_{n_1} \otimes P_{0,1}^{(n_2)} & & \\ & & -\mathbb{1}_{n_1} \otimes P_{-1,0}^{(n_2)} & \\ & & & -\mathbb{1}_{n_1} \otimes P_{-1,1}^{(n_2)} \end{pmatrix}. \tag{2.62}$$

Remember that $n_1 = d/2$ and $n_2 = (d-2)/2$. The operators $P_{i,j}^{(n)}$ are displacements of the parity operator in dimension n:

$$P_{i,j}^{(n_2)} = D_{i,j}^{(n_2)} P^{(n_2)}. \tag{2.63}$$

2.1.5 Exact solution in dimension 35

As mentioned above, in dimension 35 the Hilbert space has been exhaustively combed and we have good reason to believe that all SICs are known numerically, with very high precision. Appleby et al. (26) converted them into exact solutions. The exact solution for the fiducial labelled $35j$ is nine pages long and quite hard to read. We obtain a simpler expression for the exact fiducial labelled $35j$, using the numerical solution available in (7), after increasing its precision to 1200 digits with the aid of a program written by Appleby (27).

The numerical solution in Scott and Grassl's paper are given in a basis in which the order-3 Zauner symmetry U_{Z_d} is the unitary corresponding to the SL(2) matrix

$$Z_d = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}. \tag{2.64}$$

It is customary to express SICs in this basis, so let us call the above form of the symplectic matrix *the standard form*.

To obtain a simpler expression of the exact solution, we rotate the numeric fiducial to a carefully chosen basis, using, as before, the fact that in dimension 35 we are allowed to split the Hilbert space into a d-dimensional and a $(d-2)$-dimensional space, with $d = 7$, in accordance with Chinese Remaindering. Over the whole space, the Zauner symmetry $U_{Z_{35}}$ can be written as a tensor product of the corresponding symmetries U_{Z_7} and U_{Z_5}. The SL(2) matrix corresponding to $U_{Z_{35}}$ can be expressed in terms of the SL(2) correspondents of U_{Z_7} and U_{Z_5} in the following way:

$$\begin{pmatrix} \alpha \mod 35 & \beta \mod 35 \\ \gamma \mod 35 & \delta \mod 35 \end{pmatrix} \sim \begin{pmatrix} \alpha \mod 7 & \kappa^{-1}\beta \mod 7 \\ \kappa\gamma \mod 7 & \delta \mod 7 \end{pmatrix} \times \begin{pmatrix} \alpha \mod 5 & \kappa^{-1}\beta \mod 5 \\ \kappa\gamma \mod 5 & \delta \mod 5 \end{pmatrix}, \tag{2.65}$$

where $\kappa = \frac{d-1}{2} = 2$. The inverse of κ is taken modulo 7 in the first matrix and modulo 5 in the second.

Chinese remaindering now allows us to solve the above system for α, β, γ, and δ, according to the isomorphism 2.36. Before we do so, however, we introduce one more trick. Appleby (26) has proven that in

dimensions of the form $d = 3k+1$, the Zauner symmetry can be rotated in such a way that its corresponding SL(2) matrix has only one non-zero element per row. Such a matrix is called *monomial*. In dimension 7, the monomial form of the Zauner symmetry is

$$Z_7 = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}. \tag{2.66}$$

We use this form in equation 2.65. In dimension 5 no monomial form exist, so we keep the standard form:

$$Z_5 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}. \tag{2.67}$$

The symplectic matrix that satisfies 2.65 is then

$$Z'_{35} = \begin{pmatrix} 25 & -7 \\ 7 & 9 \end{pmatrix}. \tag{2.68}$$

To transform between Z and Z', we use the transformation matrix $T = \begin{pmatrix} -1 & -11 \\ -3 & 1 \end{pmatrix}$, together with a permutation matrix P_{CR}. We perform the permutation in order to ensure that the basis in which we end up is in lexicographic order, as a tensor product of the bases in dimension 7 and 5.

$$U'_{Z_{35}} = P U_T U_{Z_{35}} U_T^\dagger P^{-1}. \tag{2.69}$$

In the above, U_T is the unitary corresponding to the symplectic T. We are now in a basis where the order-three unitary symmetry of 35-dimensional SICs is composed, via Chinese remaindering, from the 7x7 and 5x5 unitaries that serve as symmetries for SICs in dimensions 7 and 5 respectively, with the 7x7 one expressed in monomial form. It is onto this basis that we rotate the SIC $35j$, with the aid of matrices U_T and P.

The Zauner symmetry $U'_{Z_{35}}$ splits the 35-dimensional Hilbert space into three subspaces, of dimensions 12, 12, and 11, corresponding to eigenvalues ω_3, ω_3^2, and 1, respectively. The $|35j\rangle$ fiducial is to be found in the small eigenspace of the Zauner symmetry, with eigenvalue 1. We can obtain this eigenspace by taking the tensor product between the appropriate eigenspaces of the 7-dimensional Zauner symmetry with eigenspaces of the 5-dimensional Zauner symmetry (minding that the total eigenvalue is 1). The Zauner symmetry splits the 7-dimensional Hilbert space into two spaces of dimension 2 (with eigenvalues ω_3 and

ω_3^2, respectively) and one space of dimension 3 (with eigenvalue 1). Similarly, the 5-dimensional Hilbert space is split into two 2-dimensional spaces (with eigenvalues ω_3 and ω_3^2, respectively) and one 1-dimensional space (with eigenvalue 1). We further split these subspaces using the parity operator, $P_{ij}^d = \delta_{i,d-j}^{(d)}$. The superscript on the Kronecker delta indicates that it is evaluated modulo d. The parity operator has eigenvalues ± 1.

We thus obtain the following eigenvectors in dimension 7:

- Zauner eigenvalue ω_3^2

$$|\omega_3^2, +\rangle_7 = \frac{1}{\sqrt{6}} \begin{pmatrix} 0 \\ 1 \\ +\omega_3^2 \\ +\omega_3 \\ +\omega_3 \\ +\omega_3^2 \\ 1 \end{pmatrix} \qquad |\omega_3^2, -\rangle_7 = \frac{1}{\sqrt{6}} \begin{pmatrix} 0 \\ 1 \\ +\omega_3^2 \\ -\omega_3 \\ +\omega_3 \\ -\omega_3^2 \\ -1 \end{pmatrix} \tag{2.70}$$

- Zauner eigenvalue ω_3

$$|\omega_3, +\rangle_7 = \frac{1}{\sqrt{6}} \begin{pmatrix} 0 \\ 1 \\ \omega_3 \\ \omega_3^2 \\ \omega_3^2 \\ \omega_3 \\ 1 \end{pmatrix} \qquad |\omega_3, -\rangle_7 = \frac{1}{\sqrt{6}} \begin{pmatrix} 0 \\ 1 \\ \omega_3 \\ -\omega_3^2 \\ \omega_3^2 \\ -\omega_3 \\ -1 \end{pmatrix} \tag{2.71}$$

- Zauner eigenvalue 1

$$|1\rangle_7 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |1, +\rangle_7 = \frac{1}{\sqrt{6}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \quad |1, -\rangle_7 = \frac{1}{\sqrt{6}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ -1 \\ 1 \\ -1 \\ -1 \end{pmatrix} \tag{2.72}$$

The values inside the ket represent the eigenvalues, first with respect to the Zauner symmetry, then with respect to the parity operator.

The eigenvectors in $d = 5$ are:

- eigenvalue 1

$$|1\rangle_5 = \frac{1}{N_{f_4}}\omega_5|f_4\rangle, \qquad |f_4\rangle = \begin{bmatrix} \omega_5+\omega_5^4 \\ \omega_5+\omega_5^2 \\ \omega_5^3+\omega_5^4 \\ \omega_5^3+\omega_5^4 \\ \omega_5+\omega_5^2 \end{bmatrix} \tag{2.73}$$

- eigenvalue ω_3:

$$|\omega_3,+\rangle_5 = \frac{1}{N_{f_0}}|f_0\rangle, \quad |f_0\rangle = \begin{pmatrix} 4-2\omega_5^3+2\omega_3(\omega_5^2-\omega_5^3) \\ \omega_5^2+\omega_5^3+\omega_3(2\omega_5^2+2\omega_5^3+\omega_5^4) \\ 4\omega_5+3\omega_5^3+3\omega_3(\omega_5^3-\omega_5^4) \\ 4\omega_5+3\omega_5^3+3\omega_3(\omega_5^3-\omega_5^4 \\ \omega_5^2+\omega_5^3+\omega_3(2\omega_5^2+2\omega_5^3+\omega_5^4) \end{pmatrix}$$

$$|\omega_3,-\rangle = \frac{\omega_5}{N_{f_1}}|f_1\rangle, \qquad |f_1\rangle = \begin{pmatrix} 0 \\ \sqrt{5}\omega_3+\omega_5-\omega_5^3 \\ -\omega_5^4+1 \\ \omega_5^4-1 \\ -\sqrt{5}\omega_3-\omega_5+\omega_5^3 \end{pmatrix}$$

- eigenvalue ω_3^2:

$$|\omega_3^2,+\rangle_5 = \frac{1}{N_{f_2}}\omega_5|f_2\rangle, \quad |f_2\rangle = \begin{pmatrix} 4-2\omega_5^3+2\omega_3^2(\omega_5^2-\omega_5^3) \\ \omega_5^2+\omega_5^3+\omega_3^2(2\omega_5^2+2\omega_5^3+\omega_5^4) \\ 4\omega_5+3\omega_5^3+3\omega_3^2(\omega_5^3-\omega_5^4) \\ 4\omega_5+3\omega_5^3+3\omega_3^2(\omega_5^3-\omega_5^4 \\ \omega_5^2+\omega_5^3+\omega_3^2(2\omega_5^2+2\omega_5^3+\omega_5^4) \end{pmatrix}$$

$$|\omega_3,-\rangle_5 = \frac{1}{N_{f_3}}\omega_5|f_3\rangle, \qquad |f_3\rangle = \begin{pmatrix} 0 \\ \sqrt{5}\omega_3^2+\omega_5-\omega_5^3 \\ -\omega_5^4+1 \\ \omega_5^4-1 \\ -\sqrt{5}\omega_3^2-\omega_5+\omega_5^3 \end{pmatrix}.$$

By N_{fi} we mean the norm of $|fi\rangle$.

We obtain the following basis for the relevant eigenspace of $U'_{Z_{35}}$:

$$
\begin{aligned}
&|e_1\rangle = |1\rangle_7 \otimes |1\rangle_5, && |e_2\rangle = |1,+\rangle_7 \otimes |1\rangle_5,\\
&|e_3\rangle = |1,-\rangle_7 \otimes |1\rangle_5, && |e_4\rangle = |\omega_3,+\rangle_7 \otimes |\omega_3^2,+\rangle_5\\
&|e_5\rangle = |\omega_3,-\rangle_7 \otimes |\omega_3^2,+\rangle_5, && |e_6\rangle = |\omega_3,+\rangle_7 \otimes |\omega_3^2,-\rangle_5,\\
&|e_7\rangle = |\omega_3,-\rangle_7 \otimes |\omega_3^2,-\rangle_5, && |e_8\rangle = |\omega_3^2,+\rangle_7 \otimes |\omega_3,+\rangle_5,\\
&|e_9\rangle = |\omega_3^2,-\rangle_7 \otimes |\omega_3,+\rangle_5, && |e_{10}\rangle = |\omega_3^2,+\rangle_7 \otimes |\omega_3,-\rangle_5,\\
&|e_{11}\rangle = |\omega_3^2,-\rangle_7 \otimes |\omega_3,-\rangle_5.
\end{aligned}
$$

In this basis, the SIC fiducial $|35_j\rangle$ is, up to an overall phase:

$$
\begin{aligned}
|35j\rangle = e^{i\nu_2}(&\sqrt{p_2}|e_2\rangle - i\sqrt{p_3}|e_3\rangle)\\
&+\sqrt{p_4}|e_4\rangle + \sqrt{p_5}e^{i\nu_5}e^{i\nu_3}|e_5\rangle\\
&+e^{i\nu_8}(\sqrt{p_8}|e_8\rangle + \sqrt{p_9}e^{i\nu_9}|e_9\rangle),
\end{aligned}
\tag{2.74}
$$

The absolute values p_i of the components are:

$$
\begin{aligned}
p_2 &= \frac{1}{12}(1+2\sqrt{2}) & p_5 &= \frac{1}{6}(3-\sqrt{2})\\
p_3 &= \frac{1}{12}(3-2\sqrt{2}) & p_8 &= \frac{1}{6}(-1+\sqrt{2})\\
p_4 &= \frac{1}{6}(1-2\sqrt{2}) & p_9 &= \frac{1}{6}(3-\sqrt{2}),
\end{aligned}
\tag{2.75}
$$

together with $p_0 = p_6 = p_7 = p_{10} = p_{11} = 0$. The phases are:

$$
e^{i\nu_2} = -\frac{(-1)^{1/3}}{70}\Big(-11-27\sqrt{2}-3i\sqrt{3(123-22\sqrt{2})}\Big)^{1/6},
$$

$$
e^{i\nu_5} = \frac{1}{7}\sqrt{5-24\sqrt{2}-2i\sqrt{6(51+10\sqrt{2})}},
$$

$$
\begin{aligned}
e^{i\nu_8} = (-1)^{2/3}&\Big(\frac{1}{280}\Big)^{\frac{1}{3}}\Big(-3\sqrt{6(123-22\sqrt{2})(5-\sqrt{5})}+(11+27\sqrt{2})(1+\sqrt{5})\\
&+2i\Big(8929+871\sqrt{5}-594\sqrt{2}(-1+\sqrt{5})\\
&\quad+3\sqrt{459888\sqrt{5(3+\sqrt{5})}+1008486(5+\sqrt{5})}\Big)^{\frac{1}{2}}\Big)^{\frac{1}{3}}.
\end{aligned}
$$

We had set out to obtain compact and reader-friendly expression, and the above is so.

However, in the form above, we cannot, with the computational means available, check whether the solution is indeed a SIC, as the number field is too large. Appleby et al (17) have a definite conjecture for the simplest number field in which a SIC can be constructed, for each dimension d, and we are interested in expressing our solution in the corresponding number field in dimension 35. These number fields can be constructed using algorithms implemented in Magma (27).

To achieve this, we first take the normalization factors out of $|e_i\rangle$ and collect them, together with the $\sqrt{p_i}$'s and the phases e^{ν_i}, in the coefficients z_i:

$$|35j\rangle = \sum_{i=1}^{11} z_i |e'_i\rangle, \tag{2.76}$$

where the vectors $|e'_i\rangle$ are the tensor product of unnormalized vectors in dimensions 7 and 5. The normalization factors are $1/\sqrt{6}$ in dimension 7 and $1/Nf_{0,1,2,3,4}$ in dimension 5.

We then, using Mathematica's functions RootApproximant and MinimalPolynomial, find the minimal polynomial with integer coefficients of each z_i. We then factor the minimal polynomials over the desired number field, and thus obtain a more manageable form of the SIC. This form, however, is not reader friendly.

The number field of the coefficients z_i is the abelian extension of $\mathbb{Q}$ over a, r_1,b_1, c_1,c_2, m_1, and m_2.

$$\begin{aligned} a &= \sqrt{2} & r_1 &= \sqrt{5} \\ b_1 &= \sqrt{350 + 140 * r_1} & c_1 &= 2\cos\frac{\pi}{7}, \end{aligned} \tag{2.77}$$

c_2 is a solution of

$$x_a^3 - 3675 * x_a - 33075 * a - 13475 == 0,$$

and $m_1 = \sqrt{-2a-1}$ and $m_2 = \sqrt{2a-1}$.

3. Certification using the Elegant Bell Inequality

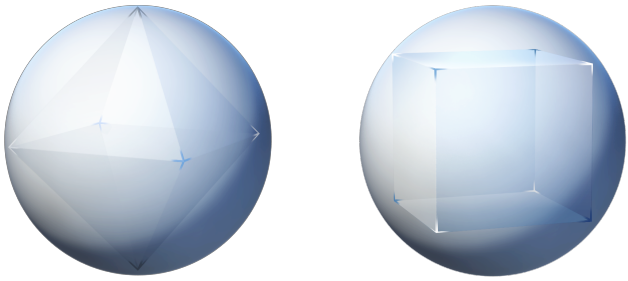
We now move on to an application of the SIC-POVMs, namely the Elegant Bell Inequality. This Bell inequality was discovered by Gisin as a bipartite inequality that is maximally spread in the Hilbert space of the measurements in the two labs of Alice and Bob (28). The elegance in the name refers to the elegant geometric structure of the measurements on the Hilbert spaces of the two parties. On Alice's side, the measurements consist of three mutually unbiased bases, while on Bob's side the measurements consist of two sets of symmetric informationally-complete POVMs, or SICs. The measurements on both sides are represented in Figure 3.1. Notice that the picture on Bob's side is similar to 2.1.

The accompanying papers III and IV are on the topic of device independent certification using this inequality.

In quantum communication and quantum security, as there are many protocols and tasks that become more interesting for real-life applications if we assume that there are untrustworthy parties involved.

Paper III deals with the question of whether the EBI is *self-testing*. Self-testing designates the property, exhibited by some Bell inequalities, of allowing the maximal quantum violation to only occur in a unique way. Put more simply, if we had a black box that claimed to produce a state and to perform correlation measurements corresponding to a Bell inequality, and we used it to violate the Bell inequality and found maximal violation, than we would be able to conclude unequivocally which quantum state was involved and which measurements were performed. We prove that the EBI is not self-testing in the strict sense.

A mathematical definition of self-testing has been around for a few years, proposed by McKague(29), and Paper III proves that the EBI does not satisfy it. However, we show that the inequality comes very close to self-testing, and maximal violation of it gives an almost complete picture of the black box device. The difficulty in completing the picture can be traced back to the problem of distinguishing an operator from its complex conjugate. Similar difficulties in fulfilling the requirements of self-testing had been reported by others (29; 30). In the wake of our



(a) The octahedron in Alice's Bloch sphere.

(b) The cube in Bob's Bloch sphere.

Figure 3.1: Measurements on Alice's side (on the left) and Bob's side (on the right). The state involved in the EBI consists of two entangled qubits, so the Hilbert space on each side is the Bloch sphere. Measurements on Alice's side define the corners of a regular octahedron inscribed in the sphere. Measuremements on Bob's side correspond to center of the faces of this octahedron and thus define its dual, a cube. The eight corners of the cube correspond to two sets of SIC-POVMs, one represented in blue, the other in white. The figure is taken from Accompanying Paper III.

publication of Paper III, a spirited discussion about the definition of self-testing, in particular whether it should be relaxed to allow for the equivalence of complex conjugated measurements, was started within the community (31). There exist now ongoing efforts to agree on a definition of self-testing that captures the usefulness of the EBI.

Paper IV deals with randomness certification, another process which is important for quantum information protocols when the manufacturer of the devices cannot be trusted (32). Random numbers are necessary in many high-stakes situations, from encryption protocols to lottery draws, so there exist strong incentives to create ever more secure random numbers generators. In addition, we need to develop tools to certify that the numbers we are using are *truly* random and not seemingly random numbers given out by a malicious party. Quantum random number generators are a promising application of quantum mechanics, as they use the intrinsic randomness of quantum systems to solve a practical task. On top of that, it has been proven, by D'Ariano *et al.* (33), that quantum randomness can be certified even if one does not trust the devices. They have also proven that the maximum number of bits that can be certified in a device-independent way from one bit of entanglement is upper bounded by *two*.

Recently, Acín *et al.* (34) have proven that this maximum can be saturated. They constructed two protocols for achieving the maximum: the first uses a simultaneous maximal quantum violation of *three* Clauser-Horne-Shimony-Holt (CHSH) Bell inequalities and is proven analytically, the second uses the maximal violation of an Elegant Bell inequality and is supported in their paper only by numerical evidence.

This is the context for our work on this problem: accompanying paper IV in this thesis proposes a modified version of this second randomness certification protocol and offers an analytic proof of certification. This protocol is the simpler of the two proposed by (34), and indeed the simplest protocol currently known for the certification of two bits of randomness from an entangled qubit. Our randomness certification in Paper IV is framed in terms of two tests that need to be passed by an ensemble of a source and measurement devices. It has recently been used by Yuan et al (35) as a test in their experiment, using photons as the physical support. It also served as inspiration for Smania et al.'s experimental certification of an informationally-complete quantum measurement (36), which also uses photons as the physical support.

In the following, I will offer an introduction to Bell inequalities and self-testing that should be sufficient for the reader to follow the attached papers.

3.1 Bell inequalities

Bell proved in 1964 that quantum mechanics makes predictions that are incompatible with any theory satisfying local realism(37) (while "locality" is somewhat intuitive, "realism" is a difficult concept to incorporate into the description of a theory. We will give a technical definition of realism, sufficient for our purposes, later). Bell's proof consisted of finding an example of a linear function of probabilities that is upper bounded by any theory that assumes local realism and showing that quantum mechanics allows for larger values of the function. It follows that quantum mechanics is incompatible with either locality or realism. The term "Bell inequality" is now used for any linear function of probabilities that is bounded tighter in local realist theories than in quantum ones. Quantum mechanics does not, in general, allow for arbitrarily large violations of these inequalities; there exists a "quantum bound" as well.

From here on, we consider only Bell inequalities involving probabilities generated by two spatially-separated observers, Alice and Bob, performing dichotomic measurements on a shared system. Many-partite

Bell inequalities exist, as well as Bell inequalities for measurements with more than two outcomes, but we don't loose any intuition by restricting to this simple case. In the following discussion, we follow Brunner et al's comprehensive review of Bell inequalities (38).

Let Alice have at her disposal n measurement settings, and Bob have m. Each party chooses a setting, let's say A_i for Alice and B_j for Bob. Let a and b denote the outcomes of Alice and Bob respectively. The joint probability of reading outcomes a and b when measurements A_i and B_j have been performed in a run of the experiment is then denoted as:

$$p(ab|A_iB_j).$$

The expectation value of a pair of operators is the sum of such probabilities over all outcomes:

$$E(A_iB_j) = \sum_{a,b} ab \cdot p(ab|A_iB_j) \tag{3.1}$$

The expectation value is also often denoted as $\langle A_iB_j \rangle$, or E_{ij}.

Realism is the assumption that in each run of the experiment $E(A_iB_)$ has a value, even if it's not measured. We will from now on assume, for the sake of simplicity, that realism holds and that it is locality that is violated by quantum mechanics.

There exist a total of $4mn$ such joint probabilities (iterating all possible settings $m*n$, and all four possible outcomes). We call the set

$$\mathbf{p} = \{p(ab|A_iB_j)\}$$

of all these probabilities *a behavior*, following (39) and (38). The space of all behaviors is $\mathcal{P} \subset \mathbb{R}^{4mn}$, defined by the possibility constraints $p(ab|A_iB_j) \geq 0, \forall a, b, i, j$ and the normalization constraints $\sum_{a,b} p(ab|A_iB_j) = 1, \forall i, j$.

There are three types of constraints within this set that have physical meaning: non-signaling behaviors, quantum behaviors, and local realist behaviors. The question of certification in our applications can be formulated as the question of whether the behavior of our system is quantum. We define each constraint below, and give a geometric interpretation of the space of all behaviors, again following (38), but also (40).

Non-signaling correlations

The non-signaling constraint (first formalized in (41)) is that the marginal probabilities of one of the parties be independent of the other's

measurement setting:

$$\sum_b p(ab|A_iB_j) = \sum_b p(ab|A_iB_k)$$

$$\sum_a p(ab|A_iB_j) = \sum_a p(ab|A_kB_j). \tag{3.2}$$

The physical interpretation is clear: Bob cannot signal to Alice by his choice of input. Non-signaling behaviors are consistent with relativity; if Alice and Bob are space-like separated they cannot use their Bell system to communicate instantaneously.

The set of non-signaling correlations is denoted $\mathcal{NS}$.

Local correlations

Locality, in intuitive terms, means that each probability in the behavior can be expressed in terms of two independent probabilities, one depending solely on Alice's measurements and outcomes, the other solely on Bob's. We can formalize the definition of locality in the context of hidden variables theory.

A hidden variables theory usually assumes that there exist some other variables, λ, on which the outcomes a and b depend. These hidden variables can account for the correlations between Alice's and Bob's experiments by having a joint causal influence on the two. The full expression of the probability is $p(ab|A_iB_j, \lambda)$. Locality then means that the behavior factorizes:

$$p(ab|A_iB_j, \lambda) = p(a|A_i, \lambda)p(b|B_j\lambda). \tag{3.3}$$

A more subtle definition of locality takes into the account that λ may involve physical quantities that are not controllable in an experiment, which makes it impossible for statistics to be collected for a fixed λ. The hidden-variable is then allowed to vary across the runs according to a distribution function $f(\lambda)$, and the behavior can be written by integrating over all values of λ:

$$p(ab|A_iB_j) = \int_\lambda f(\lambda)p(a|A_i, \lambda)p(b|B_j\lambda)d\lambda \tag{3.4}$$

The set of local correlations, which we denote $\mathcal{L}$, is strictly smaller than the set of non-signaling correlations $\mathcal{NS}$.

Quantum correlations

To define quantum behaviors, we need to define a *state* ρ_{AB} shared by the two parties, and *measurement operators*, $M_{a|A_i}$ and $M_{b|B_j}$, acting on the total Hilbert space of the system, $M_{a|A_i} : \mathcal{H} \to \mathcal{H}$ and $M_{b|B_j} : \mathcal{H} \to \mathcal{H}$. A quantum behavior, then, is any behavior for which a state and two sets of operators, as defined above, can be found such that:

$$p(ab|A_iB_j) = Tr(\rho_{AB} M_{a|A_i} M_{b|B_j}). \tag{3.5}$$

Tsirelson's problem asks whether the maximal violation of a Bell inequality is the same in scenarios where we only impose that Bob's operators and Alice's operators commute, $[M_{a|A_i}, M_{b|B_j}] = 0$, as in scenarios where we impose that Alice's operators act only on Alice's space, $M_{a|A_i} = M^A_{a|A_i} \otimes \mathbb{1}$ and Bob's operators act only on Bob's space, $M_{b|B_j} = \mathbb{1} \otimes M^B_{b|B_j}$. Tsirelson settled it in the affirmative for finite dimensional Hilbert spaces only (42). It has recently been claimed (43) that in infinite-dimensional spaces this is not the case. We restrict here, once again[1], to finite-dimensional Hilbert spaces.

In finite dimensional Hilbert spaces, any mixed state can be "purified" by going to a larger Hilbert space. We can thus, without loss of generality, take the state to be pure and the operators to be projectors. The expression of the probability then becomes:

$$p(ab|A_iB_j) = \langle \Psi | M_{a|i} \otimes M_{b|j} | \Psi \rangle. \tag{3.6}$$

Any quantum behavior satisfies the non-signaling constraint, but there exist non-signaling behaviors that are not quantum (for example, the Popescu-Rohrlich box, see (41)). Moreover, any local behavior admits a quantum description of the form 3.5, as shown for example by Pitowsky (44), but there exist quantum behaviors which are not local.

3.1.1 The Clauser-Horne-Shimony-Holt inequality

We will illustrate these constraints with the help of the most famous Bell inequality, namely the Clauser-Horne-Shimony-Holt (CHSH) inequality (45). The CHSH inequality involves two settings for Alice and two settings for Bob. Let us take the eigenvalues of both A_i and B_j to be ± 1, and let E_{ij} denote the expectation value for measurement

[1] Remember we restricted to finite-dimensional spaces in order to keep the Weyl-Heisenberg groups discrete in chapter 2.

settings i and j respectively:

$$E_{ij} = \langle A_i B_j \rangle = \sum_{a,b} ab \cdot p(ab|A_i B_j). \tag{3.7}$$

The inequality then reads:

$$S = E_{00} + E_{01} + E_{10} - E_{11} \leq 2, \tag{3.8}$$

with 2 being the maximum value of S allowed by local realist theories.

The maximum quantum value is

$$S = 2\sqrt{2} > 2. \tag{3.9}$$

Equation (3.9) illustrates the content of Bell's theorem, establishing the non-local character of quantum theory. All bipartite Bell inequalities that involve two dichotomic measurements on both parties are equivalent (up to permutations of inputs and outputs) to the CHSH (45).

We will now prove the bounds of CHSH. To prove the local bound we assign values to the expectation values of the operators, maximizing S. We keep in mind that, for local behaviors, it holds that $\langle A_i B_j \rangle = \langle A_i \rangle \langle B_j \rangle$. There are 4^2 possible assignments, and to find the maximum value one needs simply to go over them (see Table 3.3). But it is easy to see that the value $S = 2$ cannot be exceeded. We maximize the terms that come into S with a plus sign by assigning the value $+1$ to each A_i and B_j, thus maximizing each term. Since the last term, $A_1 B_1$, which comes into S with a minus sign is also 1, the total value of S is 2 in this scenario. If we, on the contrary, minimize the negative term, by assigning opposite sign values to A_1 and B_1, the positive term is also minimized, and the total value of S is again 2.

We can now revisit the notion of realism and get a more intuitive grasp of it. Realism is the assumption that each entry of this table has a truth value in each run of the experiment, regardless of which column is actually measured. If realism does not hold, then it becomes meaningless to speak of S as a linear combination of these expectation values.

In quantum mechanics, we can choose a state and some operators such that, when plugging them in equation (3.5), we obtain a behavior that violates the CHSH inequality. I will give an example of such a choice here (in Section 3.2.1 we will see that this choice is in fact essentially unique, but for now let us treat this as a generic example). Let us take the state to be the singlet state of two qubits, $|\Psi\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, and Alice's operators to be $A_0 = Z_A$ and $A_1 = X_A$, where Z_A and X_A

$\langle A_0 \rangle$	$\langle A_1 \rangle$	$\langle B_0 \rangle$	$\langle B_1 \rangle$	E_{00}	E_{01}	E_{10}	E_{11}	S
1	1	1	1	1	1	1	1	2
1	1	1	−1	1	−1	1	−1	2
1	1	−1	1	−1	1	−1	1	−2
1	1	−1	−1	−1	−1	1	1	−2
1	−1	1	1	1	1	−1	−1	2
1	−1	1	−1	1	−1	−1	1	−2
1	−1	−1	1	−1	1	1	−1	2
1	−1	−1	−1	−1	−1	1	1	−2
−1	1	1	1	−1	−1	1	1	−2
−1	1	1	−1	−1	1	1	−1	2
−1	1	−1	1	1	−1	−1	1	−2
−1	1	−1	−1	−1	−1	1	1	−2
−1	−1	1	1	−1	−1	−1	−1	2
−1	−1	1	−1	−1	1	−1	1	−2
−1	−1	−1	1	1	−1	1	−1	2
−1	−1	−1	−1	1	1	1	1	2

Table 3.1: the local values of S

are the Pauli operators acting on Alice's Hilbert space, in the z and x directions, respectively. We choose Bob's operators to be:

$$B_0 = \frac{-Z_B - X_B}{\sqrt{2}} \qquad B_1 = \frac{-Z_B + X_B}{\sqrt{2}}, \tag{3.10}$$

where Z_B and X_B are the corresponding Pauli operators on Bob's Hilbert space. We then have $\langle A_0 B_0 \rangle = \langle A_0 B_1 \rangle = \langle A_1 B_0 \rangle = 1/\sqrt{2}$ and $\langle A_1 B_1 \rangle = -1/\sqrt{2}$. Putting these values together in S, we get $S = 2\sqrt{2} > 2$, at odds with (3.8). We have shown that quantum mechanics *allows* for the value $2\sqrt{2}$, thus proving Bell's theorem.

In order to prove that $2\sqrt{2}$ is indeed the maximum value allowed by quantum mechanics, we start by defining the operator

$$F = A_0 B_0 + A_0 B_1 + A_1 B_1 - A_1 B_1. \tag{3.11}$$

Since the eigenvalues of A_i (and B_j) are ± 1, it follows the operators are all involutions, i.e. they all square to the identity: $A_i^2 = \mathrm{I}_A$ and $B_j^2 = \mathrm{I}_B$. Using this, we have

$$F^2 = 4\mathrm{I}_{AB} - [A_0, A_1][B_0, B_1]. \tag{3.12}$$

We also need to define the norm of an operator O, as following:

$$\|O\| = \sqrt{\langle O^\dagger O \rangle}, \tag{3.13}$$

or simply

$$\|O\| = \sqrt{\langle O^2 \rangle}, \tag{3.14}$$

since we are only concerned with Hermitian operators. Plugging the following norm inequalities:

$$\|[A_0, A_1]\| \leq 2\|A_0\|\|A_1\| \tag{3.15}$$

$$\|[B_0, B_1]\| \leq 2\|B_0\|\|B_1\| \tag{3.16}$$

into equation (3.12), and using the fact that $\langle A_i \rangle \leq 1$ and $\langle B_i \rangle \leq 1$, the quantum limit follows.

Non-signaling theories allow for higher values of S, see (41). The authors introduce blackbox devices, nowadays called Popescu-Rohrlich boxes (or PR boxes) characterized by the fact that they allow for maximum violation of the CHSH inequality in a non-signaling way. To obtain the maximum non-signaling violation of the CHSH inequality we are no longer bound by quantum mechanics to obey (3.5), that is, to use self-adjoint operators on the Hilbert space as measurement settings. If the four expectation values present in S are completely independent, they can be chosen as: $\langle A_0 B_0 \rangle = \langle A_0 B_1 \rangle = \langle A_1 B_0 \rangle = 1$ and $\langle A_1 B_1 \rangle = -1$. The total value of S is then four.

Geometric Interpretation

The sets of local, quantum, and non-signaling scenarios ($\mathcal{L}$, $\mathcal{Q}$, $\mathcal{NS}$, respectively) are all closed, bounded, and convex. In general, we have the strict inclusion $\mathcal{L} \subset \mathcal{Q} \subset \mathcal{NS}$, and it has been shown that $dim\mathcal{L} = dim\mathcal{Q} = dim\mathcal{NS}$ (46). A convex set can be defined as the hull of a set of extremal points. Equivalently, any point in the set can be written as a convex combination of the extremal points. If the set of extremal points is finite, then the set is a convex polytope. Both the set of non-signaling behaviors and the set of local realist behaviors are convex polytopes. The set of quantum probabilities is a convex set, but not a polytope, i.e. it has an infinite number of extremal points. The hyperplanes delimiting the local set correspond to Bell inequalities.

Vertesi et al. have studied the geometry of the probability sets in a recent paper (40). They classified the relations between the faces of $\mathcal{L}$, $\mathcal{Q}$, and $\mathcal{NS}$, and concluded that seven distinct cases can occur. Figure

3.2, based on their results, illustrates all the possible cases in one slice of the polytope. It may be the case, however, that no actual slice contains all types of boundaries. The classification is based on whether, for a particular Bell-type inequality, the maximal local value $\beta_{\mathcal{L}}$, the maximal quantum value $\beta_{\mathcal{Q}}$, and the maximal non-signaling value $\beta_{\mathcal{NS}}$, coincide, and on whether, if the values do coincide, the faces defined them are strictly included in one another, or are equal.

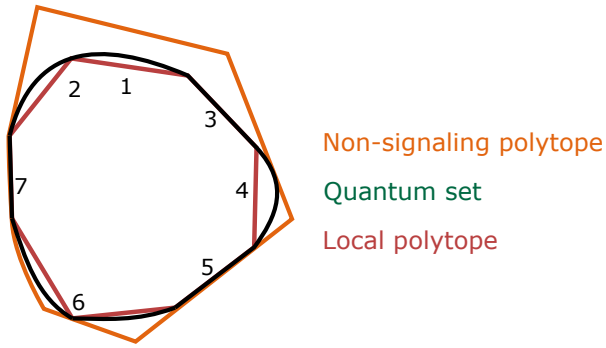


Figure 3.2: An illustration of a possible 2D slice through the set of probabilities, containing all cases of relations between the faces of the three sets of interest, for a given Bell inequality:

1. Case 1 corresponds to $\beta_L < \beta_Q < \beta_{NS}$
2. Case 2 corresponds to $\beta_L = \beta_Q < \beta_{NS}$, and the quantum face includes the local one
3. Case 3 corresponds to $\beta_L = \beta_Q < \beta_{NS}$, and the quantum face coincides to the local one
4. Case 4 corresponds to $\beta_L < \beta_Q = \beta_{NS}$, and the non signaling face includes the quantum one
5. Case 5 corresponds to $\beta_L = \beta_Q = \beta_{NS}$, the quantum face coincides to the local one, and the non-signaling face includes the quantum one
6. Case 6 corresponds to $\beta_L = \beta_Q = \beta_{NS}$, the quantum face includes the local one, and the non-signaling face includes the quantum one
7. Case 6 corresponds to $\beta_L = \beta_Q = \beta_{NS}$, the local, quantum, and non-signaling faces coincide.

A geometric aspect which this classification does not cover, but which is interesting for our purposes, is that some Bell inequalities give rise to fully dimensional faces (i.e. facets), and some Bell inequalities give rise to lower dimensional faces of the local polytope. A facet of a d dimensional polytope is $d-1$ dimensional. The CHSH inequality is one example of an inequality that determines a facet of the local polytope. The Elegant Bell inequality, with which we will deal later, describes a hyperplane which does not contain a facet. Bell inequalities of this

second type do not determine the geometry of the local polytope in a precise sense, as they can be rotated around the lower-dimensional face that they include. An illustration of this can be found in Fig.2.

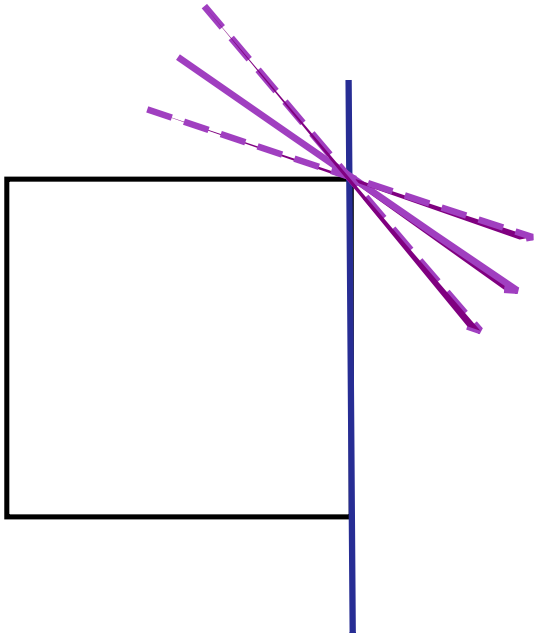


Figure 3.3: An illustration of hyperplanes containing faces of the local polytope, for the case $d = 2$. The blue line contains a facet (in this case a one dimensional surface, an edge of the square). It uniquely determines a face of the polytope. The solid purple line contains a lower dimensional face (in this case a zero dimensional face, a corner of the square). It can be rotated around the corner. The purple lines would determine equivalent Bell inequalities

To illustrate this, we look again at the CHSH inequality. To determine the dimension of the faces of the correlation polytope determined by the CHSH inequality, we follow a framework laid out by Pitowsky (47). We use a "truth-table" to go over the possible values of S, similar to Table 3.1, but setting the possible expectation values of each operator to 0 and 1, so that the formalism resembles Boolean algebra:

$\langle A_0 \rangle$	$\langle A_1 \rangle$	$\langle B_0 \rangle$	$\langle B_1 \rangle$	E_{00}	E_{01}	E_{10}	E_{11}
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0
0	0	1	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	0	0	0	0	0
0	1	0	1	0	0	0	1
0	1	1	0	0	0	1	0
0	1	1	1	0	0	1	1
1	0	0	0	0	0	0	0
1	0	0	1	0	1	0	0
1	0	1	0	1	0	0	0
1	0	1	1	1	1	0	0
1	1	0	0	0	0	0	0
1	1	0	1	0	1	0	1
1	1	1	0	1	0	1	0
1	1	1	1	1	1	1	1

Table 3.2

Take each row in the table to be a vector in eight dimensional real space. There are sixteen such vectors and they define the corners of the local polytope. Given an eight dimensional vector $v = (v_{A_0}, v_{A_1}, v_{B_0}, v_{B_1}, v_{E_{00}}, v_{E_{01}}, v_{E_{10}}, v_{E_{11}})$, then v corresponds to a local behavior if and only if it can be written as a linear combination of the 16 corners. In order to determine whether a given inequality defines a facet or another face, we look at the number of corners that are exactly on the face (i.e. the number of corners for which the value of S is maximal). For a d dimensional polytope the number of corners on a facet is at least d.

Remember that all inequalities with two dichotomic measurements on each side are equivalent to the CHSH. They can be expressed in terms of the vector elements as:

$$-1 \leq v_{E_{00}} + v_{E_{01}} + v_{E_{11}} - v_{E_{10}} - v_{A_0} - v_{B_1} \leq 0 \tag{3.17a}$$

$$-1 \leq v_{E_{10}} + v_{E_{11}} + v_{E_{01}} - v_{E_{00}} - v_{A_1} - v_{B_1} \leq 0 \tag{3.17b}$$

$$-1 \leq v_{E_{00}} + v_{E_{01}} + v_{E_{11}} - v_{E_{10}} - v_{A_0} - v_{B_1} \leq 0 \tag{3.17c}$$

$$-1 \leq v_{E_{00}} + v_{E_{01}} + v_{E_{11}} - v_{E_{10}} - v_{A_0} - v_{B_1} \leq 0. \tag{3.17d}$$

The number of corners that saturate each of these inequalities is 8, which means that each of the inequalities defines a facet.

3.1.2 The elegant Bell inequality

The elegant Bell inequality (EBI from here on) is a bipartite Bell inequality introduced by Gisin (28). One of the parties, Alice, chooses among three dichotomic measurement settings, while the other party, Bob, chooses among four dichotomic measurement settings, giving a total of twelve joint settings. The operator that comes into the inequality is:

$$\begin{aligned}\Sigma =& A_1B_1 + A_1B_2 - A_1B_3 - A_1B_4 + A_2B_1 - A_2B_2 \\ &+ A_2B_3 - A_2B_4 + A_3B_1 - A_3B_2 - A_3B_3 + A_3B_4.\end{aligned} \tag{3.18}$$

Using the notation $E_{k,l}$ for the mean value of the product of the outcomes of Alice's kth and Bob's l, and fixing the possible outcomes of each operator to ± 1, the EBI reads

$$\begin{aligned}S \equiv& E_{1,1} + E_{1,2} - E_{1,3} - E_{1,4} + E_{2,1} - E_{2,2} \\ &+ E_{2,3} - E_{2,4} + E_{3,1} - E_{3,2} - E_{3,3} + E_{3,4} \leq 6.\end{aligned} \tag{3.19}$$

Its maximum quantum value is $S = 4\sqrt{3} > 6$ (34).

As mentioned earlier in the chapter, the elegance in the name refers to the fact that measurements for both parties are maximally spaced out on the Hilbert space of the system (the Bloch sphere). The maximal quantum violation is achieved when Alice and Bob share a maximally entangled pair of qubits, the eigenstates of Alice's three projective measurements form a complete set of three mutually unbiased bases (MUBs), and the eigenstates of Bob's four projective measurement can be divided into two sets, each of which defines a symmetric informationally complete positive operator-valued measure (SIC-POVM).

3.2 Quantum certification

3.2.1 Self-testing

The concept of *self-testing* was introduced by Mayers and Yao (48). In their initial paper, self testing was seen as a test for a photon source that would guarantee the source's usefulness for implementing the BB84 protocol for quantum key distribution, in a secure way. In general, self testing says that if the statistics of a *real experiment* correspond to those of a *reference experiment*, then the real experiment is *effectively equivalent* to the reference experiment. An exact definition of self-testing, formalized by McKague (29; 49), is: the reference experiment is *self-testing*

if for any other experiment in which Alice performs m local measurements $A_k = \{\Pi_{\pm}^{A_k}\}$ and Bob performs n local measurements $B_l = \{\Pi_{\pm}^{B_l}\}$ on a shared state $|\psi\rangle$, a complete agreement of the two experiments statistics, i.e., equality

$$\langle \phi | \Pi_{\pm}^{a_k} \Pi_{\pm}^{b_l} | \phi \rangle = \langle \psi | \Pi_{\pm}^{A_k} \Pi_{\pm}^{B_l} | \psi \rangle \tag{3.20}$$

for all k, l, implies the existence of a local unitary, or, more precisely, a local isometric embedding

$$\begin{aligned} \Phi = \Phi_A \otimes \Phi_B : H_A \otimes H_B &\to (H_A \otimes H_a) \otimes (H_B \otimes H_b) \\ &= (H_A \otimes H_B) \otimes (H_a \otimes H_b) \end{aligned} \tag{3.21}$$

such that $\Phi(\Pi_{\pm}^{A_k} \Pi_{\pm}^{B_l} | \psi \rangle) = |\chi\rangle \otimes \Pi_{\pm}^{a_k} \Pi_{\pm}^{b_l} | \phi \rangle$, where $|\chi\rangle$ is some arbitrary but normalized vector in $H_A \otimes H_B$.
The above definition is complete, and perfectly general. We will discuss two examples, both of them using as the reference experiment the maximal violation of a Bell inequality. First, we deal with the maximal violation of the CHSH inequality, as it is the simplest example of self testing, as well as the most studied.

Self-testing property of the CHSH inequality

Popescu and Rohrlich (50) characterized all the scenarios in which the CHSH inequality is maximally violated and proved that all of them involve the presence of a maximally entangled qubit shared by the two parties, as well as the presence of generators of a Lie algebra as settings in both Alice's and Bob's experiments.

We will go over Popescu and Rohrlich's derivation, as this will allow us to get a better intuition of the strength of self-testing, then we will consider the implications of this result for self-testing. In the end of this section, we will summarize our results about the self-testing properties of the EBI, included in the accompanying Paper I.

First, we go through the derivations of the condition of maximal violation of the CHSH in quite a bit of detail. The most general description of the system is that we have a generic bipartite state, $|\Psi\rangle$, and two dichotomic operators for each party (denoted, as in the previous section, by A_0 and A_1 for Alice, and by B_0 and B_1 for Bob). Together, they maximally violate the CHSH inequality:

$$\langle \Psi | F | \Psi \rangle = \langle \Psi | A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 | \Psi \rangle = 2\sqrt{2} \tag{3.22}$$

We use the Schmidt decomposition of a pure qubit state:

$$|\Psi\rangle = \sum_{i=1}^{n} c_i |u_i v_i\rangle \tag{3.23}$$

We make minimal assumptions about the system. Namely we assume that the dichotomic measurement settings of both Alice and Bob have as eigenvalues 1 and -1, and that the Hilbert space of each particle have dimension equal to the number of terms in the decomposition (3.23). From equation (3.22), it follows that $|\Psi\rangle$ is an eigenstate of F with eigenvalue $2\sqrt{2}$: $F|\Psi\rangle = 2\sqrt{2}|\Psi\rangle$. Applying F again, we get:

$$F^2|\Psi\rangle = 8|\Psi\rangle \tag{3.24}$$

Expanding equation 3.24, and using the fact that $A_i^2 = B_j^2, \forall i, j$ we get

$$\begin{aligned}(4 &+ B_0B_1 + A_0A_1 - A_0A_1B_0B_1 + B_1B_0 + A_0A_1B_1B_0 - A_0A_1 \\ &+ A_1A_0 + A_1A_0B_0B_1 - B_0B_1 - A_1A_0B_1B_0 - A_1A_0 - B_1A_0)|\Psi\rangle \\ &= 8|\Psi\rangle,\end{aligned} \tag{3.25}$$

which we can express as

$$i(A_0A_1 - A_1A_0)i(B_0B_1 - B_1B_0)|\Psi\rangle = 4|\Psi\rangle, \tag{3.26}$$

Since the eigenvalues of A_0 and A_1 are ± 1, the eigenvalues of $(A_0A_1 - A_1A_0)$ cannot exceed 2 in absolute value, and the same is true for $(B_0B_1 - B_1B_0)$. It follows that

$$\begin{aligned}(i[A_0, A_1])^2|\Psi\rangle &= -(A_0A_1A_0A_1 - A_0A_1A_1A_0 - A_1A_0A_0A_1 + A_1A_0A_1A_0) \\ &= (2 - (A_0A_1A_0A_1 + A_1A_0A_1A_0))|\Psi\rangle \\ &= 4|\Psi\rangle,\end{aligned} \tag{3.27}$$

which implies

$$(A_0A_1A_0A_1 + A_1A_0A_1A_0)|\Psi\rangle = -2|\Psi\rangle, \tag{3.28}$$

and therefore

$$\langle\Psi|(A_0A_1 + A_1A_0)^2|\Psi\rangle = 0, \tag{3.29}$$

which means that $|\Psi\rangle$ is an eigenvector of $A_0A_1 + A_1A_0$ with eigenvalue 0. From the decomposition (3.23) it follows that each term $|u_1\rangle ... |u_n\rangle$ is an eigenvector of $A_0A_1 + A_1A_0$ with eigenvalue 0. Since we have

assumed the dimension of H_A to be n, it follows that $A_0A_1 + A_1A_0$ must be identically zero:

$$A_0A_1 + A_1A_0 = 0. \tag{3.30}$$

Equation (3.30) implies that A_0 and A_1 are two of the generators of an $SU(2)$ algebra. A similar result can be obtained about B_0 and B_1. Thus maximum violation of the CHSH inequality implies something quite strong about the measurements of the two parties. Furthermore, we can derive a conditions on the coefficients of the state as well, from the decomposition

$$|\,\Psi\,\rangle = \sum_{ij=1}^{n/2} c_{ij}|\,\alpha_{ij}\,\rangle. \tag{3.31}$$

The state needs to be a generalized singled state. We then get a description of the most general experiment that can maximally violate the CHSH inequality, and the fact that this turns out to be a rather specific experiment is the essence of selftesting. It is this derivation of which states and measurements maximally violate the CHSH inequality that constitutes the starting point of discussions about self testing.

Incidentally, Mayers and Yao's result (48), also concerns the singlet. It was McKague (29; 49) who put these two results in terms of equivalence of experiments. Further developments were produced by Wang et al. (51), who found a criteria for discerning if a bipartite Bell inequality with two dichotomic observables for each party certifies the existence of the singlet. Their paper refers to this as "self-testing the singlet", but the term is used in an inexact way; as we have seen, "self-testing" means certification of the measurements as well.

Selt-testing property of the EBI

In our work in Paper III, we have used Popescu and Rohrlich's methods to characterize experiments that maximally violate the EBI and determine whether the maximal violation of the EBI is self testing. We have found that the EBI is not selftesting in a strict sense. It does turn out, however, that the maximal violation of the EBI always involves a singlet, and specific measurements for the two parties, as described in Section 3.1.2. EBI's failure to be fully selftesting has to do with the difficulty of discerning operators from their complex conjugates.

In order to characterize all the states and measurements that maximally violate the EBI, we start from the general scenario, similarly as for the CHSH inequality. Alice measures three dichotomic observables

A_0, A_1, A_2, Bob measures four dichotomic observables, B_0, B_1, B_2, B_3. All observables have as eigenvalues ± 1. We denote the state shared by Alice and Bob by $|\Psi\rangle$ and assume that the state together with the operators maximally violate the EBI:

$$\langle\Psi|\Sigma|\Psi\rangle = 4\sqrt{3}, \tag{3.32}$$

where Σ has been defined in Section 3.1.2. Let $|\psi\rangle = \sum_{i=1}^{m}\sum_{p=1}^{d_i}\lambda_i |u_p^i v_p^i\rangle$ be a Schmidt decomposition of $|\Psi\rangle$, with i labeling the m different Schmidt coefficients and d_i being the multiplicity of λ_i. We need to also assume that the Hilbert spaces of Alice and Bob have the same dimension N, and to define the operators

$$D_1 = (A_1 + A_2 + A_3)/\sqrt{3}, \tag{3.33a}$$
$$D_2 = (A_1 - A_2 - A_3)/\sqrt{3}, \tag{3.33b}$$
$$D_3 = (-A_1 + A_2 - A_3)/\sqrt{3}, \tag{3.33c}$$
$$D_4 = (-A_1 - A_2 + A_3)/\sqrt{3}. \tag{3.33d}$$

We can then conclude the following things about the states and operators that satisfy (3.32):

- Alice's observables anticommute: $\{A_k, A_l\} = 2\delta_{kl}$. From this it follows that the space $\mathcal{H}_A$ can be split into orthogonal subspaces

$$\mathcal{H}_A^i = \bigoplus_{p=1}^{n_i} \mathcal{H}_A^{ip}, \qquad A_k^i = \bigoplus_{p=1}^{n_i} A_k^{ip}. \tag{3.34}$$

  In each subspace, Alice's operators can be written, in some basis, like this:

$$A_1^{ip} = Z, \qquad A_2^{ip} = X, \qquad A_3^{ip} = \pm Y. \tag{3.35}$$

- Bob's space can be split in the same way:

$$\mathcal{H}_B^i = \bigoplus_{p=1}^{n_i} \mathcal{H}_B^{ip}, \qquad B_l^i = \bigoplus_{p=1}^{n_i} B_l^{ip}, \tag{3.36}$$

  and the operators admit the decomposition:

$$B_1^{ip} = \tfrac{1}{\sqrt{3}}(A_1^{ip} + A_2^{ip} - A_3^{ip}) = \tfrac{1}{\sqrt{3}}(Z + X \mp Y), \tag{3.37a}$$
$$B_2^{ip} = \tfrac{1}{\sqrt{3}}(A_1^{ip} - A_2^{ip} + A_3^{ip}) = \tfrac{1}{\sqrt{3}}(Z - X \pm Y), \tag{3.37b}$$
$$B_3^{ip} = \tfrac{1}{\sqrt{3}}(-A_1^{ip} + A_2^{ip} + A_3^{ip}) = \tfrac{1}{\sqrt{3}}(-Z + X \pm Y), \tag{3.37c}$$
$$B_4^{ip} = \tfrac{1}{\sqrt{3}}(-A_1^{ip} - A_2^{ip} - A_3^{ip}) = \tfrac{1}{\sqrt{3}}(-Z - X \mp Y). \tag{3.37d}$$

- the state $|\Psi\rangle$ can be represented as

$$\begin{aligned} |\psi\rangle &= \sum_{i=1}^{m}\sum_{p=1}^{n_i} \lambda_i (|0_A^{ip}0_B^{ip}\rangle + |1_A^{ip}1_B^{ip}\rangle) \\ &= \sqrt{2}\sum_{i=1}^{m}\sum_{p=1}^{n_i} \lambda_i |\phi_+^{ip}\rangle. \end{aligned} \tag{3.38}$$

The above list characterizes the most general scenario which maximally violates the EBI. The sign indeterminacy on A_3^{ip} in each subspace cannot be resolved. The implication of this indeterminacy is that the maximal violation of the EBI is not self-testing, in the strict sense of the definition in Section 3.2.1,and in the same way that the CHSH inequality is. Observing a maximal violation of the EBI does, however, tell us a lot about the state and operators involved.

3.2.2 Randomness certification

We move on now to the second type of certification addressed in this thesis: randomness certification. The characterization of randomness is not a straightforward task. Given a source of bits, one can verify the presence of apparent randomness by performing a series of tests and checking the distribution of the numbers. However, this does not safeguard against the scenario in which the numbers are in fact generated according to a preset pattern and thus known to the manufacturer of the device (52). These numbers are called pseudo-random and ruling them out is part of randomness certification. On top of these adversarial considerations, there are fundamental considerations as well. Randomness generating processes that use classical systems will be inherently non-random, as classical mechanics is deterministic. Classical randomness relies on the complexity of the pattern and the limited computational power of the adversary. Quantum mechanics is non-deterministic, which opens the way for quantum random numbers generators (QRNGs), generating *true randomness*. The first QRNG was proposed in 2000 by Gisin et al. (53) and nowadays QRNGs are commercially available.

Quantum randomness certification is device independent and relies on the presence of non-local correlations. This immediately tells us that Bell inequalities can be used for such tasks. The question of how much randomness can be certified from a certain amount of non-local correlations arise naturally. It has been settled by D'Ariano *et al.* (33), who have proven that the maximum number of bits that can be certified in a device-independent way from one bit of entanglement is upper

bounded by *two*. Recently, Acín *et al.* (34) have proven analytically that this maximum can be *saturated*. They proved this by constructing two protocols for achieving the maximum; the first uses a simultaneous maximal quantum violation of *three* Clauser-Horne-Shimony-Holt (CHSH) Bell inequalities, the second uses the maximal violation of an Elegant Bell inequality and is supported only by numerical evidence. The second is the simpler protocol of the two (and indeed the simplest protocol currently known for the certification of two bits of randomness from an ebit).

This is the context for our work on this problem: accompanying Paper IV in this thesis proposes a modified version of this second randomness certification protocol and offers an analytic proof of the certification. Our randomness certification, in Paper IV, is framed in terms of two tests that need to be passed by an ensemble of a source and measurement devices.

The scenario is the following: Alice has a source of systems and a measurement device with four outcomes. She uses them to perform a 4-outcome measurement, A_4, on each system produced by the source. The generated outcomes are apparently unpredictable, i.e., after many measurements Alice notices that the four outcomes appear with the same frequency and follow no pattern. However, it may be the case that an adversary, let's call it Eve, can guess the outcomes. Eve could even be the manufacturer of the source, which means that the device is not trusted. Here the concept of device-independent certification comes in: Alice needs a way of testing her randomness without trusting the production of the device. Such a test will naturally be independent on the nature of the device, or on any model that we may use to describe the device.

The tests we proposed, if passed, certify that Alice's device generates numbers which are unpredictable for everyone, i.e. Eve's guessing probability cannot exceed 1/4, which is what she would get by chance. The tests involve a third party, Alice's trusted collaborator Bob, who has access to a second system produced by Alice's source (see Fig. 1 of the accompanying Paper IV).

We model Eve's guessing as the application of a local 4-outcome POVM F (if Eve reads out a she guesses that Alice rad out a). Then Eve's local guessing probability is defined as the probability that Eve makes a correct guess given that Alice measures A_4 and Eve measures F, and is denoted by G:

$$G = \max_F \sum_a P(a, a|A_4, F). \tag{3.39}$$

For the tests, Alice needs three additional dichotomic measurements, A_1, A_2, A_3, and Bob needs four dichotomic measurements, B_1, B_2, B_3, B_4. The system is in a total state $|\Psi\rangle$, belonging to $\mathcal{H}_A \otimes; H_B \otimes \mathcal{H}_E$, where $\mathcal{H}_A$, $\mathcal{H}_B$, $\mathcal{H}_E$ are the Hilbert spaces of Alice, Bob, and Eve, respectively. We also introduce the notation $E_{a|i,j} = \sum_b b\mathrm{p}(ab|A_i B_j)$, for the expectation value of Bob's jth measurement conditioned on the outcome of Alice's ith measurement.

The first test is a Bell test. Alice's and Bob's observables, together with their state, should maximally violate the EBI, when plugged into (3.18). That is, $S = 4\sqrt{3}$, where S is defined in (3.19).

The proof relies on the self-testing properties of the EBI. We saw earlier the maximal violation of the elegant Bell inequality can only happen under some very specific conditions, that restrict the state and the measurements on both parties (up to conjugation). The first test is therefore a quantumness witness for the source.

The second test requires the existence of a family of four qubit operators $Q = \{Q_a\}$:

$$Q_a = \gamma_a^0 \mathbb{I} + \gamma_a^1 Z + \gamma_a^2 X + \gamma_a^3 Y, \tag{3.40}$$

where Z, X, Y are the Pauli operators and

$$\gamma_a^0 = P(a|A_4), \tag{3.41a}$$
$$\gamma_a^1 = \tfrac{\sqrt{3}}{2}(E_{a|4,1} + E_{a|4,2}), \tag{3.41b}$$
$$\gamma_a^2 = \tfrac{\sqrt{3}}{2}(E_{a|4,1} + E_{a|4,3}), \tag{3.41c}$$
$$\gamma_a^3 = -\tfrac{\sqrt{3}}{2}(E_{a|4,2} + E_{a|4,3}). \tag{3.41d}$$

The test is passed if $\mathrm{p}(a|A_4) = 1/4$ and Q_a are linearly independent one-dimensional projectors. For a 4-outcome qubit POVM such as Q_a, this condition is equivalent to being an extremal POVM, or a POVM that cannot be written as a linear combination of other POVMs (33). The reader may find it interesting that, just like the probabilities illustrated earlier, POVMs form a convex set. In Paper IV the test is formulated in terms of extremality of the POVM.

Q_a are one-dimensional projectors if $\mathrm{tr}Q_a > 0$ and $\det Q_a = 0$. The trace condition is satisfied if $P(a|A_4) > 0$ and the determinant is satisfied if

$$(E_{a|4,1} + E_{a|4,2})^2 + (E_{a|4,1} + E_{a|4,3})^2 + (E_{a|4,2} + E_{a|4,3})^2 = \frac{4}{3} P(a|A_4)^2, \tag{3.42}$$

for all a. Finally, the condition of linear independence is satisfied if the matrix of coditional expectations values

$$\begin{pmatrix} E_{1|4,1} & E_{1|4,2} & E_{1|4,3} \\ E_{2|4,1} & E_{2|4,2} & E_{2|4,3} \\ E_{3|4,1} & E_{3|4,2} & E_{3|4,3} \end{pmatrix} \tag{3.43}$$

has full rank.

The proof that these tests together amount to certifications of two bits of information is detailed in Paper IV.

3.2.3 Conclusion

The two studies in this chapter help illustrate that SICs are of interest not only for their geometric and number theoretical properties, but also for more practical purposes. The two certifications that we presented here rely on a Bell inequality that, in its turn, relies on the presence of maximally spread quantum measurements.

While there are other, simpler, ways to certify the existence of the maximally entangled two-qubit state, the self-testing properties of the Bell inequality enable in addition the certification of three measurements on one side and of a set of four measurements on the other side.

The protocol for randomness certification presented in this thesis and in the attached Paper IV constitutes the simplest, in terms of number of measurements involved, method of saturating the bound of randomness that can be certified from one bit of entanglement. This does not necessarily mean that the protocol would be the best candidate for experimental implementation, as other Bell inequalities may be easier to violate (54) and four-outcome POVMs, like the one required by this protocol, are hard to implement (55). However, as stated in the beginning of this chapter, the protocol has been used as inspiration for experimental implementations, by Yuan et al (35) and by Smania et al. (36).

Acknowledgements

I am grateful to Ingemar, who has given me both freedom and structure, and has been a great supervisor in all aspects. I have learned a lot from you, both about physics and about how to do research in general. Perhaps the most important thing I learned is how to not get lost when faced with masses of information, how to find a roadmap through them and impose a structure.

Thank you to Ole for being a great colleague and friend. I have enjoyed working with you at every stage of our projects, from bouncing ideas, to looking for a missing sign among many pages of calculations, to sorting out what manual of style the journals want us to follow for quotation marks.

I also want to thank Marcus Appleby, Hulya Yadsan-Appleby, and Markus Grassl for our ongoing collaboration, for sharing their notes and code with me. Your warmth and support make the SIC-POVM field such a pleasant and friendly community.

Thank you to my secondary supervisor Jonas and to my mentor Michael for taking on these roles and being my backup structure, and to Mohammed for giving me a glimpse of the experimental world.

The group I visited in Poland taught me a lot of quantum information and, more importantly, helped renew my enthusiasm at a time when it was hard to see the big picture; thank you, Deba and Anubhav.

I am also very grateful to Mercedes and Gonzalo, who had an open mind about being paired with a stranger for a joint history&physics project. Our work together was a very fun part of my PhD.

I am very grateful to Isa, Åsa, Petra, and everyone in the administration of Fysikum for answering many questions and for making sure I didn't fall through the cracks. Thank you also to Sten and Per-Erik for making sure I stayed on track with my studies.

Thank you to Markus Hennrich and Maria Hermanns for being on my pre-defence committee and giving me very useful feedback, and Marcin Pawłowski for doing the same at my licentiate defence.

My colleagues in KOMKO have been a big part of making this PhD an enjoyable experience, I will miss our zoom fika! Thank you Hans

and Eddie for being such thoughtful group leaders. Many thanks to Sreekant, Iman, Axel, Jonas K., Krishanu, Supriya, Babak, Christian, Carlos, Sören, Theresa, Thomas, Themis, Ahmed, Elisabet, and Flore. I thank my colleagues and friends in KIKO as well, for our lunch group and our many conversations.

Pil and David, who lived through the pandemic and isolation with *me-while-writing*, deserve special mention. Dealing with this deadline was nowhere as stressful as I had feared; this is in large part thanks to yous. Pil also proofread this thesis and let me know when things were hard to follow, as well as providing me with snacks, entertainment, and the much-appreciated chance to work on something else occasionally. Thank you! not only for the past few months but for our friendship over the years too.

My shut-up-and-write online group(s) alleviated alienation and made putting this thesis together fun. Pernille proofread and gave valuable feedback.

I was lucky that Massi shared my deadlines to the day and I could ask for advice and information all the time; but even outside this context he is one of my go-to people for sanity-checks. Michele opens his house for me at all hours of night and day, and Vani always listens. I am also very thankful to Fabian, Gerard, Colin, Sreyashi, and Joana for a friendship that made Stockholm home. Maria and Costi for keeping me on my toes intellectually, in their different ways. Andreea, Mihael, and Olfa, who visited me in Stockholm often and stayed in touch despite the distance. Collective thanks go to Desert Island and Dezarticulat.

My aunt Florina has put out many fires over the years; she has also taught me to put them out myself. Together with my mother, she has taught me all I know on a personal level about being a researcher. Thank you also to my other aunts, uncles and cousins, in Timisoara and Canada, and to my grandpa, for always encouraging and helping me in my plans.

I owe my mother and my father all the confidence and pride that I have. My mother has also taught me to be lucid in tense situations and to like change; very useful skills for doing a PhD, but they will last me beyond that. Thank you for your support and inspiration.

I am so grateful for Vlad, who always lends me his vision when mine gets stuck. Even about physics, even about academia. Thank you for everything.

Claudia and Mickey, for the never-ending conversations that help place this work into a larger context, both in the world and in my life.

References

[1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information. Tenth anniversary edition.* Cambridge University Press, 2010. 2, 5

[2] A. J. Scott. **Tight informationally complete quantum measurements**. *J. Phys. A*, **39**, 2006. 2

[3] A. J. Scott J. M. Renes, R. Blume-Kohout and C. M. Caves. **Symmetric informationally complete quantum measurements**. *J. Math. Phys.*, **45**:2172, 2004. 5

[4] J. J. Benedetto and M. Fickus. **Finite normalized tight frames**. *Adv. Comp. Math.*, **18**(2-4), 2003. 7

[5] G. Zauner. **Quantendesigns. Grundzüge einer nichtkommutativen Designtheorie, PhD thesis (German), Quantum Designs: Foundations of anoncommutative Design Theory**. *Int. J. Quant. Inf.*, **9**, 2011. 7, 14

[6] A. Roy and A. J. Scott. **Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements**. *J. Math. Phys*, **48**(7), 2007. 7

[7] A. J. Scott and M. Grassl. **Symmetric informationally complete positive-operator valued measures: A new computer study**. *J. Math. Phys*, **51**(4), 2010. 8, 14, 15, 26

[8] M. Grassl and A. J. Scott. **Private communication**. 8

[9] M. Grassl and A. J. Scott. **Fibonacci-Lucas SIC-POVMs**. *J. Math. Phys*, **58**(12), 2017. 8

[10] H. Zhu. **SIC POVMs and Clifford groups in prime dimensions.** *J. Phys. A: Math. and Theoretical*, **43**(30), 2010. 8

[11] H. Weyl. *The theory of groups and quantum mechanics. Second edition.* Dover Publications, 1930. 9, 10

[12] E. Scholz. **Weyl entering the new quantum mechanics discourse**. *Proceedings of the Conference on the History of Quantum Physics, Berlin, German*, 2007. 9

[13] G. McConnell M. Appleby, S. Flammia and J. Yard. **SICs and algebraic number theory**. *Foundations of Physics*, **47**(8), 2017. 10

[14] D. M. Appleby. **Symmetric informationally complete positive-operator valued measures and the extended Clifford group**. *J. Math. Phys.*, **46**(5), 2005. 11, 12, 13, 24

[15] A. J. Scott. **SICs: Extending the list of solutions.** *arXiv preprint*, **arXiv:1703.03993**, 2017. 14, 18

[16] H. Yadsan-Appleby D.M Appleby and G. Zauner. **Galois automorphisms of a symmetric measurement**. *Quant. Inf. Comput.*, **13**, 2013. 16

[17] G. McConnell M. Appleby, S. Flammia and J. Yard. **Generating ray class fields of real quadratic fields via complex equiangular lines**. *Acta Arith.*, **192**, 2020. 16, 31

[18] G. McConnell. **private communication**. 17

[19] A. J. Scott. **Private communication**. 18

[20] D. Gross. **Hudson's theorem for finite-dimensional quantum systems**. *J. Math. Phys.*, **47**(12), 2006. 19

[21] M. Appleby and I. Bengtsson. **Simplified exact SICS**. *J. Math. Phys.*, **60**(6), 2019. 19

[22] S. Brierley M. Grassl D. Gross D. M. Appleby, I. Bengtsson and J.-Å. Larsson. **The monomial representations of the Clifford group**. *Quant. Inf. Comput.*, **12**, 2012. 19

[23] M. Appleby. **Unpublished notes**. 20

[24] S. Brierley Å. Ericsson M. Grassl D. M. Appleby, I. Bengtsson and J.-Å. Larsson. **Systems of imprimitivity for the Clifford group**. *Quant. Inf. Comp.*, **14**, 2014. 22

[25] D. Yakymenko V. Ostrovskyi and. **Geometric properties of SIC-POVM tensor square**. *arXiv preprint*, **arXiv:1911.05437**, 2019. 23

[26] S. Flammia M. Appleby, T. Y. Chien and S. Waldron. **Constructing exact symmetric informationally complete measurements from numerical solution**. *Journal of Physics A: Mathematical and Theoretical*, **51**(16), 2018. 26

[27] M. Appleby. **Private comunication**. 26, 31

[28] N. Gisin. **Bell inequalities: Many questions, a few answers**. In W. C. Myrvold and J. Christian, editors, *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony*, The Western Ontario Series in Philosophy of Science. Springer, The Netherlands, 2009. 33, 46

[29] M. McKague and M. Mosca. **Generalized self-testing and the security of the 6-state protocol**. In V. M.Kendon W. van Dam and S. Severini, editors, *Theory of Quantum Computation, Communication, and Cryptography, Lecture Notes in Computer Science*, **6519**, page 113. Springer, Berlin, 2010. 33, 46, 49

[30] J. Kaniewski. **Self-testing of binary observables based on commutation**. *Phys. Rev. A*, **95**(6), 2017. 33

[31] J. Kaniewski. **private communication**. 34

[32] S. Massar A. B. de La Giroday D.N. Matsukevich P. Maunz S. Pironio, A. Acín and C. Monroe. **Random numbers certified by Bell's theorem**. *Nature*, **464**(7291), 2010. 34

[33] P. L. Presti G. M. D'Ariano and P. Perinotti. **Classical randomness in quantum measurements**. *J. Phys. A: Math. Gen.*, **38**(26), 2005. 34, 51, 53

[34] T. Vértesi A. Acín, S. Pironio and P. Wittek. **Optimal randomness certification from one entangled bit**. *Phys. Rev. A*, **93**(4), 2016. 35, 46, 52

[35] Y. Xu W. Wang Y. Ma F. Zhang X. Yuan, K. Liu and X. Ma. **Experimental quantum randomness processing using superconducting qubits**. *Phys. Rev. Let.*, **117**(1), 2016. 35, 54

[36] M. Nawareg M. Pawlowski A. Cabello M. Smania, P. Mironowicz and M. Bourennane. **Experimental device-independent certification of a symmetric, informationally complete, positive operator-valued measure**. *Optica*, **7**(2), 2020. 35, 54

[37] J. S. Bell. *Einstein-Podolsky-Rosen Experiments in Quantum Mechanics, High Energy Physics And Accelerators: Selected Papers Of John S Bell (With Commentary)*. World Scientific Publishing, 1995. 35

[38] S. Pironio V. Scarani N. Brunner, D. Cavalcanti and S. Wehner. **Bell nonlocality**. *Reviews of Modern Physics*, **86**(2), 2014. 36

[39] B. Tsirelson. **Quantum Bell-type inequalities**. *Hadronic Journal Supplement*, **8**, 1993. 36

[40] E. Wolfe T. Vértesi X. Wu Y. Cai Y.-C. Liang K. T. Goh, J. Kaniewski and V. Scarani. **Geometry of the set of quantum correlations**. *Phys. Rev. A*, **97**(2), 2018. 36, 41

[41] S. Popescu and D. Rohrlich. **Quantum nonlocality as an axiom**. *Foundations of Physics*, **24**(3), 1994. 36, 38, 41

[42] V. B. Scholz and R. F. Werner. **Tsirelson's problem**. *arXiv preprint*, **arXiv:0812.4305**, 2008. 38

[43] T. Vidick J. Wright Z. Ji, A. Natarajan and H. Yuen. **Mip*= re**. *arXiv preprint*, **arXiv:2001.04383**, 2020. 38

[44] I. Pitowsky. **The range of quantum probability**. *J. Math. Phys.*, **27**(6), 1986. 38

[45] A. Shimony J. F. Clauser, M. A. Horne and R. A. Holt. **Proposed Experiment to Test Local Hidden Variable Theories**. *Phys. Rev. Let.*, **24**(10), 1970. 38, 39

[46] S. Pironio. **Lifting Bell inequalities**. *J. Math. Phys.*, **46**(6), 2005. 41

[47] I. Pitowsky. **From George Boole to John Bell-The Origins of Bell's Inequality**. In M. Kafatos, editor, *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, Fundamental Theories of Physics, page 37. Springer, Dordrecht, 1989. 44

[48] D. Mayers and A. Yao. **Quantum cryptography with imperfect apparatus**. In *Proceedings of the 39th IEEE Conference on Foundations of Computer Science, Palo Alto, CA, 1998*. IEEE, New York, 1998. 46, 49

[49] M. McKague. *Quantum Information Processing with Adversarial Devices*. University of Waterloo, 2010. 46, 49

[50] S. Popescu and D. Rohrlich. **Which states violate Bell's inequality maximally?** *Phys. Lett. A*, **169**(6), 1992. 47

[51] X. Wu Y. Wang and V. Scarani. **All the self-testings of the singlet for two binary measurements.** *New Journal of Physics*, **18**(2), 2016. 49

[52] A. Ekert and R. Renner. **The ultimate physical limits of privacy**. *Nature*, **507**(7493), 2014. 51

[53] O. Guinnard L. Guinnard A. Stefanov, N. Gisin and H. Zbinden. **Optical quantum random number generator**. *Journal of Modern Optics,*, **47**(4), 2000. 51

[54] R. D. Gill. **Statistics, causality and Bell's theorem**. *Statistical Science*, **29**(4), 2014. 54

[55] E. S. Gómez D. Cavalcanti O. Jiméne Farcías A. Acín S. Gómez, A. Mattar and G. Lima. **Experimental nonlocality-based randomness generation with nonprojective measurements**. *Phys. Rev. A*, **97**(4), 2018. 54

Paper I

Dimension towers of SICs. I. Aligned SICs and embedded tight frames

Cite as: J. Math. Phys. **58**, 112201 (2017); https://doi.org/10.1063/1.4999844
Submitted: 11 August 2017 . Accepted: 28 October 2017 . Published Online: 29 November 2017

Marcus Appleby, Ingemar Bengtsson, Irina Dumitru, and Steven Flammia

JOURNAL OF MATHEMATICAL PHYSICS **58**, 112201 (2017)

Dimension towers of SICs. I. Aligned SICs and embedded tight frames

Marcus Appleby,[1] Ingemar Bengtsson,[2] Irina Dumitru,[2] and Steven Flammia[1,3]

[1]*Centre for Engineered Quantum Systems, School of Physics, University of Sydney, Sydney, Australia*

[2]*Stockholms Universitet, AlbaNova, Fysikum, Stockholm, Sweden*

[3]*Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Received 11 August 2017; accepted 28 October 2017; published online 29 November 2017)

Algebraic number theory relates SIC-POVMs in dimension $d > 3$ to those in dimension $d(d-2)$. We define a SIC in dimension $d(d-2)$ to be aligned to a SIC in dimension d if and only if the squares of the overlap phases in dimension d appear as a subset of the overlap phases in dimension $d(d-2)$ in a specified way. We give 19 (mostly numerical) examples of aligned SICs. We conjecture that given any SIC in dimension d, there exists an aligned SIC in dimension $d(d-2)$. In all our examples, the aligned SIC has lower dimensional equiangular tight frames embedded in it. If d is odd so that a natural tensor product structure exists, we prove that the individual vectors in the aligned SIC have a very special entanglement structure, and the existence of the embedded tight frames follows as a theorem. If $d-2$ is an odd prime number, we prove that a complete set of mutually unbiased bases can be obtained by reducing an aligned SIC to this dimension. *Published by AIP Publishing.* https://doi.org/10.1063/1.4999844

I. INTRODUCTION

It sometimes happens that an apparently simple question leads into very deep waters. We are concerned with just such a question here.[1,2] To begin at the beginning, a SIC (also known as a SIC-POVM or as a maximal complex equiangular tight frame) is a collection of d^2 unit vectors in $\mathbf{C}^d$ such that they resolve the identity

$$\sum_{I=1}^{d^2} |\psi_I\rangle\langle\psi_I| = d\mathbb{1}, \tag{1}$$

and such that the absolute values of the overlaps $\langle\psi_I|\psi_J\rangle$ are equal (to $1/\sqrt{d+1}$ in fact) whenever $I \neq J$. The acronym SIC stands for Symmetric Informationally Complete and betrays the quantum state tomographical origin of the concept. In the 'Bloch space'—the affine space of Hermitian operators with unit trace equipped with the Hilbert-Schmidt inner product—a SIC is a maximal regular simplex, inscribed in the set of pure states. An obvious question is: Do SICs exist in all dimensions?

At the outset the SIC existence problem shows almost no structure. However, the known solutions make it clear that SICs are deeply implicated in a major open question in algebraic number theory. In every dimension that has been studied so far[3–6] there are SICs which are orbits under the discrete Weyl–Heisenberg group, a group with many applications in quantum mechanics,[7] in radar and communication,[8] and in some approaches to Hilbert's 12th problem.[9] Remarkably, in every known example, in the preferred basis singled out by the Weyl–Heisenberg group the components of the SIC vectors belong to abelian extensions of a real quadratic number field.[10] (We assume throughout that $d > 3$ and the SIC is Weyl–Heisenberg covariant.) Which real quadratic field that comes into play depends, contingent on a conjecture,[11] in a known way on the dimension d. After a highly non-trivial

but well understood extension of the quadratic field, one arrives at a ray class field with conductor d (or $2d$ if d is even), and it appears that this always suffices to construct a SIC in dimension d.[11] See Ref. 12 for an account that assumes little or no background in number theory. Ray class fields are important because every abelian extension is contained in some ray class field. In many (presumably most) dimensions several unitarily inequivalent SICs exist, and further extensions of the ray class field are needed to construct them all.

This particular connection between number theory and a simple geometric question was unexpected. It may be worthwhile to recall the connection between the geometry of regular polygons and the roots of unity. In number theoretic language, the roots of unity generate extensions of the rational numbers, called cyclotomic fields. They are abelian extensions because the Galois group of the extension is abelian.[13] Moreover the cyclotomic field generated by an nth root of unity is a ray class field over the rational number field $\mathbb{Q}$, with conductor n.[14] The importance of the conductor is that one cyclotomic field is a subfield of another if the conductor of the one divides the conductor of the second. Every abelian extension of the rational numbers is a subfield of one of these ray class fields.

A more pertinent example may be that of mutually unbiased bases (MUB) in dimensions d such that d is a prime number. Complete sets of such bases can be constructed using the Weyl–Heisenberg group, and in the preferred basis singled out by the group, the components of all the MUB vectors can be constructed using dth roots of unity only (with a slight complication for $d = 2$).[15] Thus, to construct MUB in d dimensions, one needs cyclotomic fields with conductor d. Keep in mind that the roots of unity look extremely complex if one expresses them in terms of nested radicals, but they appear simple once it is realized that they can be obtained by evaluating the transcendental function $e^{2\pi iz}$ at rational points. (See Appendix A.) SICs are two orders of magnitude more difficult because the relevant number fields are not yet fully understood. In particular, a description making use of special values of transcendental functions is conspicuously missing. Finding such a description forms an important part of the unsolved 12th problem on Hilbert's famous list. We say "two orders of magnitude" because there is a completed theory of abelian extensions of imaginary quadratic fields, one order of magnitude more difficult than the theory of the cyclotomic fields, and relying on the geometry of elliptic curves. Hilbert is reported as saying that this theory "is not only the most beautiful part of mathematics but also of all science."[16] But he wanted more, and understanding abelian extensions of the real quadratic fields seems a natural next step.

We have reached the deep waters. To see how the dimension towers arise out of them, we need to add some details. The real quadratic field $\mathbb{Q}(\sqrt{D})$ conjectured to be relevant to SICs in dimension d consists of the set of all numbers of the form $x + \sqrt{D}y$, where x and y are rational numbers and[10]

$$D = \text{square-free part of } (d+1)(d-3). \tag{2}$$

Starting from this real quadratic number field one may perform further extensions to reach the ray class fields with conductor d (or $2d$ if d is even).

The next question is what dimensions d correspond to what square-free integers D. To see this, one fixes a square free integer $D > 1$ and solves the Diophantine equation

$$(d+1)(d-3) = m^2 D \quad \Leftrightarrow \quad (d-1)^2 - m^2 D = 4 \tag{3}$$

for the integers m and d. The solution consists of infinite sequences in each case.[11,12] The beginnings of the sequences corresponding to the first three values of D are

$$d = 7, 35, 199, 1155, 6727, 39203, 228487 \ldots \quad \text{corresponding to} \quad D = 2, \tag{4}$$

$$d = 5, 15, 53, 195, 725, 2703, 100\,85 \ldots \quad \text{corresponding to} \quad D = 3 \tag{5}$$

$$d = 4, 8, 19, 48, 124, 323, 844, \ldots \quad \text{corresponding to} \quad D = 5. \tag{6}$$

The last of these sequences is noteworthy for the fact that it contains no less than seven dimensions less than 1000, and is the subject of an important recent study by Grassl and Scott.[17]

As with the cyclotomic fields, one field is a subfield of another if the conductor of the first divides the conductor of the other. Consequently, the divisibility properties of the dimensions give rise to an intricate partially ordered set ordered by field inclusions.[11,12] See Fig. 1. Its structure is the same for

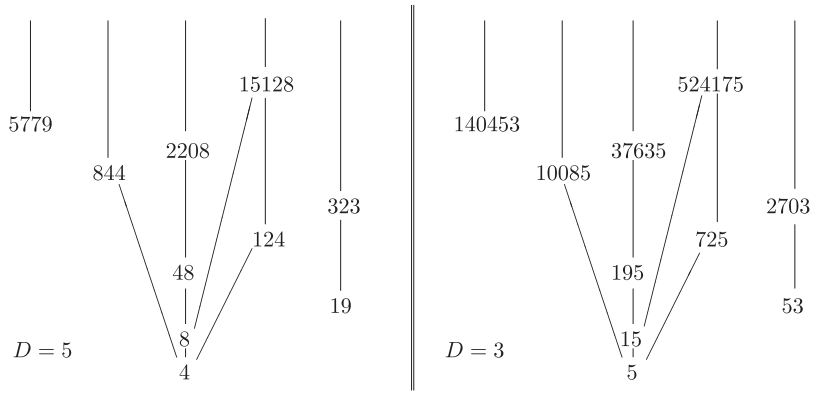


FIG. 1. Ray class field inclusions for $D = 5$ and $D = 3$. A field at the upper end of a line contains the field at the lower end. When d is even, the conductor equals $2d$, but this does not affect the links. The intricate structure of the partially ordered set does not come through because only the ten lowest dimensions are shown. In this paper, we will be concerned with the vertical connections only.

each D. For instance, the first dimension in every sequence divides the second but not the third. In this paper we will be concerned with subsequences of the form $d_1, d_2, \ldots$ with the property $d_{j+1} = d_j(d_j - 2)$ for all j. It is easily seen that the elements of such subsequences correspond to the same value of D. In fact, if $N = d(d-2)$ then

$$(N+1)(N-3) = (d^2 - 2d + 1)(d^2 - 2d - 3) = (d-1)^2(d+1)(d-3). \tag{7}$$

The square-free part is $(d+1)(d-3)$. Since d divides N, the ray class field with conductor d is a subfield of that with conductor N. The replacement $d \to d(d-2)$ thus generates an infinite "tower" (or "ladder") of ray class fields over the same real quadratic field, each one contained in the next. Examples of towers of this form include

$$7 \to 35 \to 1155 \to \cdots \quad \text{corresponding to} \quad D = 2, \tag{8}$$

$$5 \to 15 \to 195 \to \cdots \quad \text{corresponding to} \quad D = 3, \tag{9}$$

$$4 \to 8 \to 48 \to \cdots \quad \text{corresponding to} \quad D = 5. \tag{10}$$

As a glance at Fig. 1 makes clear, there are other towers (such as $4 \to 124 \to 15\ 128 \to \cdots$) not considered here.

When translated into Hilbert space, this means that the number field from which one constructs d-dimensional SICs embeds into that used to construct $d(d-2)$-dimensional SICs. We are then led to ask how this number theoretic embedding manifests itself in terms of the geometry of the Hilbert space. This question was first addressed by Gary McConnell, who studied the scalar products among SIC vectors and found that some of the overlap phases in dimension $d(d-2)$ actually belong to the smaller field. The pattern is subtle and has many facets. Here we focus on one of them: in every known example, we find that some of the overlap phases in dimension $d(d-2)$ are squares of overlap phases from dimension d or the negative thereof. The precise relationship is described in observations 1 and 2 in Sec. III. This facet has significant geometrical consequences which we explore in Secs. IV–VIII.

This relationship between the phases leads to our definition of *aligned* SICs, and we conjecture that corresponding to every SIC in dimension d there is an aligned SIC in dimension $d(d-2)$. We observe that lower dimensional equiangular tight frames (ETFs) can be found embedded in all our examples of aligned SICs, as described in Sec. IV.

We then specialize to the case of odd dimensions. We study the entanglement properties of an aligned SIC in (odd) dimension $d(d-2)$ and prove two theorems regarding the spectrum of their reduced density operators in Sec. V. We show that starting with an aligned SIC in dimension $p(p+2)$, for p an odd prime, we can obtain a full set of MUB in dimension p via an affine map; this is shown in Theorem 3 in Sec. VI. We then show in Theorem 4 in Sec. VII that an aligned SIC in

odd dimension $d(d-2)$ necessarily contains two ETFs of the kind whose existence was observed in Sec. IV. Finally, we show in Theorem 5 in Sec. VIII that such a SIC necessarily has the F_b symmetry whose existence was noted empirically by Scott and Grassl.[3,4]

Proving the even dimensional analogs of the results proven in Secs. V–VIII involves some significant complications, arising because in even dimensions d and $d-2$ are not relatively prime. This case will be discussed in a subsequent publication.

Our conclusions are given in Sec. IX, where we also comment on the very recent and important results of Grassl and Scott.[17]

II. PRELIMINARIES

A Weyl–Heisenberg SIC in dimension d is defined by a fiducial vector $|\psi_{0,0}\rangle$, from which the remaining SIC vectors $|\psi_{i,j}\rangle$ are obtained by acting with the d^2 displacement operators $D_{i,j}$. The labels are pairs of non-negative integers $0 \leq i, j < d$. For convenience these operators are often indexed by a two-component "vector" $\mathbf{p}$, and the SIC vectors are then written as $|\psi_{\mathbf{p}}\rangle = D_{\mathbf{p}}|\psi_{\mathbf{0}}\rangle$.[18] We use both notations interchangeably, guided by convenience rather than principle. Readers unfamiliar with these matters are referred to Appendix B, and readers who need to be convinced of the preferred role of the Weyl–Heisenberg group are referred to the literature.[19] In dimension 8 there exists a sporadic SIC covariant under a related Heisenberg group. See Ref. 20 for a recent discussion. It will be completely ignored here.

The *SIC overlap phases* in dimension d are defined by

$$e^{i\theta_{\mathbf{p}}} = \begin{cases} 1 & \text{if} \quad \mathbf{p} = \mathbf{0} \\ \sqrt{d+1}\,\langle \psi_{\mathbf{0}}|D_{\mathbf{p}}|\psi_{\mathbf{0}}\rangle & \text{if} \quad \mathbf{p} \neq \mathbf{0} \end{cases}. \tag{11}$$

It turns out, in every case where an exact fiducial is known, that the overlap phases are algebraic integers, and in fact algebraic units, in the number fields they give rise to 11 and 12. In this respect, they are similar to the roots of unity, which are algebraic units in the cyclotomic fields.

The importance of the Weyl–Heisenberg group derives largely from the fact that it is a unitary operator basis,[21] which means that every operator A acting on $\mathbb{C}^d$ admits a unique expansion

$$A = \sum_{\mathbf{p}} a_{\mathbf{p}} D_{-\mathbf{p}}, \quad a_{\mathbf{p}} = \frac{1}{d}\mathrm{Tr} D_{\mathbf{p}} A. \tag{12}$$

In particular, for a one-dimensional projector, this specializes to

$$|\psi\rangle\langle\psi| = \frac{1}{d}\sum_{\mathbf{p}} D_{-\mathbf{p}} \langle\psi|D_{\mathbf{p}}|\psi\rangle. \tag{13}$$

This formula will enter most of our arguments. In particular, it means that the vectors in a SIC can be reconstructed from their overlap phases.

A technicality needs to be mentioned here because it plays a large role in the intermediate stages of our argument. The choice of the fiducial vector—among the vectors in a given SIC—seems at first sight to be arbitrary so that we might just as well consider the overlap phases

$$\langle\psi_{\mathbf{q}}|D_{\mathbf{p}}|\psi_{\mathbf{q}}\rangle = \langle\psi_{\mathbf{0}}|D_{-\mathbf{q}} D_{\mathbf{p}} D_{\mathbf{q}}|\psi_{\mathbf{0}}\rangle = \omega^{\langle \mathbf{p},\mathbf{q}\rangle}\langle\psi_{\mathbf{0}}|D_{\mathbf{p}}|\psi_{\mathbf{0}}\rangle, \tag{14}$$

where ω is a dth root of unity, $\langle \mathbf{p}, \mathbf{q}\rangle$ is an integer modulo d, and we used properties of the displacement operators that are explained in Appendix B. But then the number theoretical properties of the overlap phases can get "polluted" by roots of unity. A good choice of the fiducial vector can be made by observing that the Clifford group (the unitary automorphism group of the Weyl–Heisenberg group) contains the symplectic group over the integers modulo d as a factor group. A definite copy of this group is represented by unitary operators U_F, where F is a symplectic two-by-two matrix, with entries that are integers modulo d (or $2d$ if d is even).[18] It turns out, in every case where an exact or numerical fiducial is known, that there always exist special choices of F and of the vectors such that $|\psi_{\mathbf{0}}\rangle$ is an eigenvector of U_F. Such SIC vectors are called *centred*. The SIC vector $|\psi_{\mathbf{q}}\rangle$

is left invariant by $D_{\mathbf{q}}U_F D_{-\mathbf{q}}$ and is said to be *displaced*. Centred SIC vectors are our preferred fiducial vectors because (empirically) the overlaps then lie in a smaller field, and the action of the Galois group simplifies. In dimensions divisible by 3 there is a further complication because then there are displacement operators commuting with the relevant U_F. As a result, centred SIC vectors come in triplets. It turns out, in every case where an exact fiducial is known, that one of them is singled out by the number theoretical properties of its overlap phases and is said to be *strongly centred*.[11,12]

We will need to distinguish SIC overlap phases in dimensions d from those in dimension $N = d(d-2)$. The latter are defined, using a strongly centred SIC fiducial $|\Psi_{\mathbf{0}}\rangle$ in dimension N, by

$$e^{i\Theta_{\mathbf{p}}} = \sqrt{N+1}\langle\Psi_{\mathbf{0}}|D^{(N)}_{\mathbf{p}}|\Psi_{\mathbf{0}}\rangle = (d-1)\langle\Psi_{\mathbf{0}}|D^{(N)}_{\mathbf{p}}|\Psi_{\mathbf{0}}\rangle. \tag{15}$$

Again we set $e^{i\Theta_{0,0}} = 1$ by convention. We label the operators with a superscript to signify the dimension, whenever this is demanded for clarity. The other convention established here is that capital letters Θ and Ψ are associated to the larger dimension N, whereas lower case θ and ψ refer to overlap phases and fiducials in the smaller dimension d.

Given that we know $e^{i\theta_{\mathbf{p}}}$ in dimension d, what can we say about $e^{i\Theta_{\mathbf{p}}}$ in dimension $d(d-2)$? If there is a pattern, what are the geometrical consequences? We will present some theorems concerning the second question, but for a technical reason we will restrict ourselves to the case of odd dimensions d. The reason is that the integers d and $d-2$ are relatively prime if the dimension d is odd, and then the Weyl–Heisenberg group, and indeed the whole Clifford group, splits as a direct product. The Hilbert space $\mathbb{C}^{d(d-2)}$, with d odd, is thus displayed as a tensor product $\mathbb{C}^d \otimes \mathbb{C}^{d-2}$ in a preferred way. The (known) details revolve around the Chinese remainder theorem from elementary number theory. They are spelled out in Appendix D. The tensor product structure makes it much easier to describe the geometrical consequences that we have found. In particular, we can then use the language of entanglement theory, and it is irresistible to make use of this when we can. We will prove that the entanglement properties of a SIC in $d(d-2)$ dimensions are very special if it is aligned to one in dimension d. Moreover, when $d-2$ is an odd prime number, we can include mutually unbiased bases (MUB) in the picture, and we do so in Sec. VI.

III. SQUARED PHASES IN DIMENSIONAL TOWERS

The observations that will lead to our definition of aligned SICs are summarized in Tables I and II. Every SIC in the tables is aligned to the one immediately below it (if any), in a sense to be explained. Our calculations are numerical, and the precision is limited. For $d \leq 15$ we used the numerical fiducials given by Scott and Grassl. (In five cases exact calculations have been made by Gary McConnell.)[3]

Before presenting the tables, we make an important clarifying remark. It must be understood that *none* of the phenomena we describe in this section has been proved to be a necessary consequence

TABLE I. SIC ladders with three known rungs. Exactly known SICs are in boldface, and they are underlined if they are ray class SICs. The pair 15ac is surrounded by brackets because they are constructed from the same field. The order of the symmetry group is given below the label, with an asterisk if anti-unitary symmetries are included, a subscript a if the Zauner symmetry is of the unusual kind [see Eq. (B7) for definitions], and a subscript s if the fiducial sits in the smallest of the three Zauner subspaces, as explained further in the main text.

48g	**48f**	195d	195b	195a	195c
24^*_a	6	12	6	6	6
8b	**8a**	**15d**	**15b**	(**15a**	**15c**)
12^*_s	3	6	3	3	3
4a		**5a**			
6^*		3			

TABLE II. SIC ladders with only two known rungs, with the same conventions as in the previous table.

24c	**35j**	**35i**	63b	63c	80i	99b	99c	99d	120c	120b	143a	143b	168a
6	12_s^*	6_s	6	6	6_s	6	6	6	12_a	6	6_s	6_s	6
6a	**7b**	**7a**	(**9a**	**9b**)	**10a**	**11c**	(**11a**	**11b**)	**12b**	**12a**	(**13a**	**13b**)	**14b**
3	6^*	3	3	3	3	3	3	3	6_a^*	3	3	3	3

of the definition of a SIC. Each property of SICs that we discuss in this section as being universal (i.e., holding for all SICs, assuming further yet unknown ones exist) should be read with the caveat, "in every known case." Still, the claims are based on a large number of examples. At the end of this section we will frame a definition motivated by some of them.

First, we should explain the labeling system used for SICs.[3] SICs in a given dimension fall into orbits of the extended Clifford group (see Appendix A), which includes both unitary and anti-unitary transformations. The number of such orbits varies with the dimension, in ways that are not yet understood. Every SIC is labeled by the dimension and a letter labeling the extended Clifford orbit to which it belongs.

Every SIC vector is left invariant by a subgroup of the extended Clifford group that also transforms the SIC into itself. For centred fiducials this symmetry group is a subgroup of the extended symplectic group. As suggested by a conjecture of Zauner's,[1] and confirmed in all the examples, the symmetry group always contains a cyclic subgroup of order 3. It is generated by a unitary operator called the Zauner operator.

For $d \leq 50$ the order of the symmetry group may increase with the labeling letter's position in the alphabet.[3] For higher dimensions no such system has been adopted. Then the lexicographical order reflects the order in which the various orbits were found.[4] Thus 4a is on a unique orbit in dimension 4, 48g has the highest symmetry of all SICs in dimension 48, and 63p is the last orbit that was discovered in dimension 63. If the labeling system reminds the reader of the labeling system used for spectral classes of stars (in logical order, OBAFGKM), then so be it.

A striking fact is that the order of the symmetry group doubles for each rung of the ladder in the tables. The tables contain some extra information that can be ignored for the time being: In dimensions $d = 3$ or 6 modulo 9 the symplectic group contains two different conjugacy classes of order 3 elements, represented by the matrices F_z and F_a. See Eq. (B7). SICs invariant under U_{F_z} exist in all dimensions, but if $d = 3$ modulo 9 SICs invariant under U_{F_a} exist too. Being of order 3, the Zauner operators split the Hilbert space into three Zauner subspaces. SIC vectors are always to be found in the largest of these, but in dimensions $d = 8$ modulo 9 the smallest subspace also contains SIC fiducials. There holds

$$d = 3 \text{ or } 8 \mod 9 \quad \Leftrightarrow \quad d(d-2) = 3 \mod 9, \tag{16}$$

$$d = 1 \text{ or } 4 \text{ or } 7 \mod 9 \quad \Leftrightarrow \quad d(d-2) = 8 \mod 9. \tag{17}$$

Thus the first exceptional property is "inherited" by the next rung, the second is not.

Each dimension contains a SIC known as a ray class SIC, constructed using a ray class field over the real quadratic field $\mathbb{Q}(\sqrt{D})$, where D is the square free part of the integer $(d + 1)(d - 3)$. Other SICs in the same dimension are constructed from extensions of the ray class field. More precisely, there is a unique Galois multiplet (i.e., an orbit under the joint action of the Galois group and the extended Clifford group) of SICs belonging to the same ray class field; examples where the multiplet has more than one member include 9ab and 13ab.[5] Field inclusions give rise to a partial ordering among the fields, given in Fig. 2 in the two cases where we have exact solutions available for more than one aligned SIC in the higher dimension. This pattern is not clear to us.

Our special concern in this paper is the phenomenology of squared SIC overlap phases. This can be summarized in two observations, relating some of the overlap phases in dimension $N = d(d - 2)$ to those in dimension d:

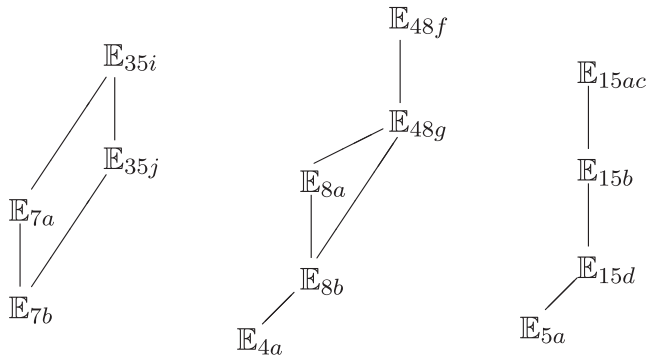


FIG. 2. Field inclusions in three of the towers. A field at an upper end of a line contains the field at the lower end. We walk up the ladders by stepping rightwards.

First observation. *For SICs in dimension d there exists a SIC in dimension* $N = d(d-2)$, *and a choice of fiducials, such that for* $\mathbf{p} = (di, dj)$, *we have*

$$e^{i\Theta_{di,dj}} = \begin{cases} +1 & \text{if} \quad d \text{ is odd} \\ -(-1)^{(i+1)(j+1)} & \text{if} \quad d \text{ is even} \end{cases}. \tag{18}$$

Second observation. *For SICs in dimensions d there exists a SIC in dimension* $N = d(d-2)$, *and a choice of fiducials, such that* $e^{i\Theta_{(d-2)i,(d-2)j}}$ *equals either plus or minus the square of an overlap phase from dimension d if d is odd. The relation between the phases is given by*

$$e^{i\Theta_{(d-2)i,(d-2)j}} = \begin{cases} -e^{2i\theta_{\alpha i+\beta j,\gamma i+\delta j}} & \text{if} \quad d \text{ is odd} \\ (-1)^{(i+1)(j+1)} e^{2i\theta_{\alpha i+\beta j,\gamma i+\delta j}} & \text{if} \quad d \text{ is even} \end{cases}. \tag{19}$$

where α, β, γ, and δ *are integers modulo d such that* $\alpha\delta - \beta\gamma = \pm 1$.

The fiducial 14a (which is in the same field as 14b[5]) does not appear in the tables because its higher dimensional cousin is not available at the moment. With this exception, the observations have been made starting from every SIC in dimension $4 \le d \le 15$. (Andrew Scott produced the fiducials 120c and 195bcd when we asked for them.)

The integers occurring in the second observation can be collected into a matrix M,

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \qquad \det M = \pm 1 \mod d. \tag{20}$$

(The arithmetic is modulo d also if d is even.) In general this is an ESL matrix belonging to some coset of the symmetry group of the SIC. One can change the coset by choosing different SICs belonging to the same Clifford orbit.

The observations hold as stated only if the SIC fiducials are centred. If a displaced fiducial is used to calculate the overlaps then $(d-2)$th roots of unity appear in $e^{i\Theta_{di,dj}}$ and dth roots of unity in $e^{i\Theta_{(d-2)i,(d-2)j}}$. If the dimension N is divisible by 3, as will always be the case from the third rung of the ladders and upwards, there are three SIC vectors in the same Zauner subspace. Unless one chooses the right one, roots of unity will again complicate the observations. It is natural to expect that the "right ones" can be taken to be strongly centred, but in those cases where an exact solution is missing we are unable to check this. Instead we refer to "suitably chosen" SIC vectors.

With this understanding, the observations hold for every adjacent pair of SICs in the columns of Tables I and II. They motivate a formal definition.

Definition. Pairs of SICs for which fiducial vectors can be chosen so that the two observations hold are aligned. The higher dimensional member of an aligned pair is called an aligned SIC.

There may well be logical dependencies among the two observations. Indeed, as we proceed, we will find some evidence that this is so. Hence a more economical statement of the definition should be possible.

Based on the fact that the two observations hold in every case we have looked at, we make the following conjecture.

Conjecture. Every d-dimensional Weyl–Heisenberg SIC has a corresponding aligned SIC in dimension $d(d-2)$.

It is worth noting that this conjecture is both stronger and weaker than the simple conjecture that SICs exist in every dimension. It posits significantly more structure on the problem and is in that sense stronger. But it allows for the possibility that some dimensions might not contain SICs, or be otherwise sporadic, while still positing the existence of infinite families. It also suggests a natural line of attack using inductive reasoning, though our own efforts in this direction have not yet been successful. But note also that the theorems in Secs. V–VIII do not depend on the conjecture. They only depend on the (non-empty) definition.

IV. EQUIANGULAR TIGHT FRAMES

Section III clearly draws attention to two special subsets of vectors in an $N = d(d-2)$ dimensional SIC, namely

$$\left\{|\Psi_{(d-2)i,(d-2)j}\rangle\right\}_{i,j=0}^{d-1} \quad \text{and} \quad \{|\Psi_{di,dj}\rangle\}_{i,j=0}^{d-3}. \tag{21}$$

The mutual overlaps within these subsets are very special numbers. What geometrical properties do these sets of vectors have?

A symmetric rank 1 POVM, also known as an equiangular tight frame (ETF), is a collection of n unit vectors in $\mathbf{C}^m$ such that they resolve the identity

$$\sum_{I=1}^{n} |\psi_I\rangle\langle\psi_I| = \frac{n}{m}\mathbb{1}, \tag{22}$$

and such that the absolute values $|\langle\psi_I|\psi_J\rangle|$ are equal whenever $I \neq J$. (We denote the dimension by m since we cannot use d, for a reason that will soon be evident.) It is easy to show that n cannot be smaller than m, and it cannot be larger than m^2.[22] A minimal ETF is an orthonormal basis and a maximal ETF is a SIC, but there are many interesting intermediate cases.[23] Because the overlaps $\langle\psi_I|\psi_J\rangle$ have constant absolute values it is easy to show—by squaring and taking the trace—that we must have

$$|\text{overlap}|^2 = \frac{n-m}{m(n-1)}. \tag{23}$$

Now let us fix an arbitrary integer $d > 3$ and ask for solutions of the Diophantine equation

$$\frac{n-m}{m(n-1)} = \frac{1}{d(d-2)+1} = \frac{1}{(d-1)^2}. \tag{24}$$

There are typically many solutions. We are interested in four of them, namely

$$(m,n) = \begin{cases} \left(d(d-2), d^2(d-2)^2\right) & \text{SIC} \\ \left(\frac{d(d-1)}{2}, d^2\right) & \text{ETF}_1 \\ \left(\frac{(d-1)(d-2)}{2}, (d-2)^2\right) & \text{ETF}_2 \\ (d-1, d) & \text{ETF}_3 \end{cases}. \tag{25}$$

The first is that of a SIC in dimension $N = d(d-2)$. The fourth is a regular simplex in dimension d. The second and third solutions have just the right number of vectors to be identified with the equiangular subsets of the N-dimensional SIC that we identified above.

The point here is that we have checked numerically, with a precision of 120 digits, that in each of the 19 aligned SICs listed in Sec. IV, the d^2 vectors in the first subset identified in (21) are linearly dependent and belong to a subspace of dimension $d(d-1)/2$. Similarly, the $(d-2)^2$ vectors in the second subset of (21) are linearly dependent and belong to a subspace of dimension $(d-1)(d-2)/2$. Hence they form smaller equiangular tight frames embedded in the aligned SIC. In the sequel, we will prove that this must happen in all aligned SICs (although the case of even d is postponed to a later publication). We will also identify special aligned SICs which contain embedded $(d-1)$-dimensional simplexes.

V. ENTANGLEMENT PROPERTIES OF SIC VECTORS

We now restrict the dimension of the Hilbert space to be odd, for the pragmatic reason that then the Weyl–Heisenberg group defines a preferred tensor product decomposition $\mathbb{C}^{d(d-2)} = \mathbb{C}^d \otimes \mathbb{C}^{d-2}$. As a result every vector in $\mathbb{C}^{d(d-2)}$ can be described in the language of entanglement theory. In particular, we will find the Schmidt decomposition very useful. Although this language is familiar to every quantum information scientist, we recall the basic facts that we need. Better explanations can be found elsewhere.[24]

Suppose that $\mathbb{C}^N = \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2}$ where $n_1 \geq n_2$. There will be local operators affecting only one of the factors of the Hilbert space. Given a pure state vector $|\Psi\rangle$ in the large Hilbert space, we define a reduced state ρ_1, which is a density matrix acting on $\mathbb{C}^{n_1}$, by the requirement that for all operators of the form $A_1 \otimes \mathbb{1}$ there holds

$$\mathrm{Tr}|\Psi\rangle\langle\Psi|(A_1 \otimes \mathbb{1}) = \mathrm{Tr}_1 \rho_1 A_1, \tag{26}$$

where Tr_1 denotes the trace over matrices acting on $\mathbb{C}^{n_1}$. This is enough to define ρ_1. One can explicitly write

$$\rho_1 = \mathrm{Tr}_2 |\Psi\rangle\langle\Psi|, \tag{27}$$

where Tr_2 denotes the partial trace over the second factor. The reduced state ρ_2 is defined similarly, using a partial trace over the first factor. Although the state we start out from is pure (defines a one-dimensional projector), the reduced state ρ_1 is typically a convex mixture of more than one pure state acting on $\mathbb{C}^{n_1}$. Generically it will have n_2 non-vanishing eigenvalues. A comfortable theorem says that the spectra of ρ_1 and ρ_2 are identical, except for additional zero eigenvalues in the larger dimension. The eigenvalues λ_k of the reduced density matrices are called Schmidt coefficients, and they completely determine the entanglement properties of a pure state $|\Psi\rangle$ in dimension $N = n_1 n_2$. Indeed, given any such pure state $|\Psi\rangle$, one can always adapt the orthonormal bases $\{|e_k\rangle\}_{k=0}^{n_1-1}$ and $\{|f_k\rangle\}_{k=0}^{n_2-1}$ in the factors such that $|\Psi\rangle$ is given by the single sum

$$|\Psi\rangle = \sum_{k=0}^{n_2-1} \sqrt{\lambda_k} |e_k\rangle |f_k\rangle . \tag{28}$$

This is called the Schmidt decomposition of the state, and the coefficients in this expansion are the positive square roots of the Schmidt coefficients. Practical computation of the Schmidt decomposition follows by noting that the singular value decomposition of the $n_1 \times n_2$ matrix whose entries are the components of $|\Psi\rangle$ gives the same information.

We can now ask: what are the entanglement properties of a SIC vector in dimension $N = d(d-2)$? For generic pure states one expects $d-2$ different, and non-vanishing, Schmidt coefficients, but we will prove that the vectors in an aligned SIC are highly non-generic in this regard.

At the outset we consider dimension $N = n_1 n_2$, where n_1 and n_2 are relatively prime and odd. We use the fact that the Weyl–Heisenberg group is a unitary operator basis, and then the group isomorphism provided by the Chinese remainder theorem, to conclude for any vector $|\Psi\rangle \in \mathbb{C}^N$ that

$$\begin{aligned} |\Psi\rangle\langle\Psi| &= \frac{1}{N} \sum_{i,j=0}^{N-1} D^{(N)}_{-i,-j} \langle\Psi| D^{(N)}_{i,j} |\Psi\rangle \\ &= \frac{1}{n_1 n_2} \sum_{i_1,j_1=0}^{n_1} \sum_{i_2,j_2=0}^{n_2} D^{(n_1)}_{-i_1,-n_2^{-1}j_1} \otimes D^{(n_2)}_{-i_2,-n_1^{-1}j_2} \langle\Psi| D^{(N)}_{i,j} |\Psi\rangle, \end{aligned} \tag{29}$$

where applying the Chinese remainder theorem (see Appendix D) allows us to express

$$\langle\Psi|D^{(N)}_{i,j}|\Psi\rangle = \langle\Psi|D^{(N)}_{i_1 n_2 n_2^{-1}+i_2 n_1 n_1^{-1},\, j_1 n_2 n_2^{-1}+j_2 n_1 n_1^{-1}}|\Psi\rangle. \tag{30}$$

If we now take the partial trace over, say, the first factor only the terms with $i_1 = j_1 = 0$ contribute. In this way, we obtain the reduced density matrix

$$\rho^{(n_2)} = \mathrm{Tr}_{n_1}|\Psi\rangle\langle\Psi| = \frac{1}{n_2}\sum_{i_2,j_2=0}^{n_2-1} D^{(n_2)}_{-i_2,-j_2}\langle\Psi|D^{(N)}_{i_2 n_1 n_1^{-1},\, j_2 n_1}|\Psi\rangle. \tag{31}$$

One summation index was shifted, which is allowed.

Now we specialize to the case of interest, namely

$$n_1 = d\,, \quad n_2 = d-2\,, \quad n_1^{-1} = n_2^{-1} = \frac{d-1}{2} \equiv \kappa, \tag{32}$$

and to the case that $|\Psi\rangle$ is a vector in an aligned SIC. We drop the subscripts on the indices—which are no longer needed since they are summation indices only—and conclude from the above that

$$\rho^{(d-2)} = \frac{1}{d-2}\sum_{i,j=0}^{d-3} D^{(d-2)}_{-i,-j}\langle\Psi|D^{(N)}_{id\kappa,jd}|\Psi\rangle. \tag{33}$$

We are now ready to prove our first theorem. The parity operator that occurs in its statement is defined in Appendix C.

Theorem 1. *If d is odd and if $|\Psi_0\rangle$ is a suitably chosen SIC vector in an aligned SIC in dimension $d(d-2)$, the density matrix reduced to dimension $d-2$ is*

$$\rho^{(d-2)}_{\mathbf{0}} \equiv Tr_d|\Psi_{\mathbf{0}}\rangle\langle\Psi_{\mathbf{0}}| = \frac{1}{d-1}(\mathbb{1}_{d-2} + P^{(d-2)}), \tag{34}$$

where $P^{(d-2)}$ is the parity operator in dimension $d-2$. Hence $\rho^{(d-2)}_{\mathbf{0}}$ is proportional to a projector from $\mathbb{C}^{d-2}$ onto a subspace of dimension $(d-1)/2$.

Proof. Recalling that we defined $e^{i\Theta_{0,0}} = 1$, we rewrite Eq. (33) as

$$\mathrm{Tr}_d|\Psi_{\mathbf{0}}\rangle\langle\Psi_{\mathbf{0}}| = \frac{1}{d-2}\left(\left(1-\frac{1}{d-1}\right)\mathbb{1} + \frac{1}{d-1}\sum_{i,j=0}^{d-3} D^{(d-2)}_{-i,-j}e^{i\Theta_{d\kappa i,dj}}\right). \tag{35}$$

The definition of an aligned SIC implies that we can choose the fiducial so that

$$e^{i\Theta_{d\kappa i,dj}} = 1\,. \tag{36}$$

Equation (35) then becomes

$$\rho^{(d-2)}_{\mathbf{0}} = \frac{1}{d-1}\left(\mathbb{1} + \frac{1}{d-2}\sum_{i,j=0}^{d-3} D^{(d-2)}_{-i,-j}\right) = \frac{1}{d-1}(\mathbb{1}_{d-2} + P^{(d-2)}), \tag{37}$$

where Eq. (C3) for the parity operator was used in the last step. In dimension $d-2$ the operator $(\mathbb{1}+P)/2$ is a projection operator of rank $(d-1)/2$, which gives the final part of the statement. □

Thus we find only $(d-1)/2$ non-vanishing Schmidt coefficients, and they are all equal. Indeed the entanglement properties of a vector belonging to an aligned SIC are very special.

The theorem applies only to aligned SICs, such as 15d and 195abcd. A calculation shows that the non-aligned fiducials 15abc have non-degenerate Schmidt coefficients, as expected for generic vectors. (Compare Table I.) On the other hand, the restriction to special choices of SIC vectors can be removed, except that one then encounters displaced parity operators on the right hand side. The proof simplifies considerably if we choose the fiducials suitably.

The next task is to find the state reduced to dimension d. From entanglement theory, we know that the spectra of $\mathrm{Tr}_d|\Psi_0\rangle\langle\Psi_0|$ and $\mathrm{Tr}_{d-2}|\Psi_0\rangle\langle\Psi_0|$ coincide. However, the precise mechanism that allows this to happen is worth studying because it depends on the details of our definition of aligned SICs. This will show that the two observations we made are in fact related.

The preliminary steps are the same as before. In Eq. (31), set $(n_1, n_2) = (d-2, d)$ and rewrite

$$\begin{aligned}\mathrm{Tr}_{d-2}|\Psi_{\mathbf{0}}\rangle\langle\Psi_{\mathbf{0}}| &= \frac{1}{d}\left(\mathbb{1} + \frac{1}{d-1}\sum_{i,j\neq(0,0)}^{d-1} D^{(d)}_{-i,-j} e^{i\Theta_{(d-2)\kappa i,(d-2)j}}\right)\\ &= \frac{1}{d}\left(\mathbb{1} + \frac{1}{d-1}\sum_{i,j\neq(0,0)}^{d-1} D^{(d)}_{2i,-j} e^{i\Theta_{(d-2)i,(d-2)j}}\right).\end{aligned} \tag{38}$$

We are now ready to bring in the squared overlap phases in dimension d by applying the full definition of an aligned SIC.

Theorem 2. *If d is odd and if $|\Psi_0\rangle$ is a suitable SIC vector in an aligned SIC in dimension $d(d-2)$, the density matrix reduced to dimension d is*

$$\rho^{(d)}_{\mathbf{0}} \equiv Tr_{d-2}|\Psi_{\mathbf{0}}\rangle\langle\Psi_{\mathbf{0}}| = \frac{1}{d-1}(\mathbb{1}_d - P^{(d)}_\theta), \tag{39}$$

where $P^{(d)}_\theta$ is a generalized parity operator in dimension d. Hence $\rho^{(d)}_0$ is proportional to a projector from $\mathbb{C}^d$ onto a subspace of dimension $(d-1)/2$.

Proof. Applying the definition of an aligned SIC to Eq. (38), we obtain

$$\begin{aligned}\rho^{(d)}_{\mathbf{0}} &= \frac{1}{d}\left(\left(1 + \frac{1}{d-1}\right)\mathbb{1} - \frac{1}{d-1}\sum_{i,j=0}^{d-1} D^{(d)}_{2i,-j} e^{2i\theta_{\alpha i+\beta j,\gamma i+\delta j}}\right)\\ &= \frac{1}{d-1}\left(\mathbb{1} - \frac{1}{d}\sum_{i,j=0}^{d-1} D^{(d)}_{-i,-j} e^{2i\theta_{-2^{-1}\alpha i+\beta j,-2^{-1}\gamma i+\delta j}}\right).\end{aligned} \tag{40}$$

We relabeled the summation index and introduced the multiplicative inverse of 2 modulo d. Making use of Eq. (20)

$$\rho^{(d)}_{\mathbf{0}} = \frac{1}{d-1}\left(\mathbb{1} - \frac{1}{d}\sum_{\mathbf{p}} D^{(d)}_{-\mathbf{p}} e^{2i\theta_{M'\mathbf{p}}}\right), \tag{41}$$

where the $GL(2,\mathbb{Z}^d)$ matrix M' obeys $\det M'^{-1} = \pm 2$. We now appeal to a result from Ref. 25, which says that, under the conditions stated, the generalized parity operator

$$P_\theta = \frac{1}{d}\sum_{\mathbf{p}} D_{-\mathbf{p}} e^{2i\theta_{M'\mathbf{p}}} \tag{42}$$

obeys $P^2_\theta = \mathbb{1}$ and has $(d+1)/2$ eigenvalues equal to $+1$ and $(d-1)/2$ eigenvalues equal to -1. □

Concerning the result from Ref. 25, we observe that it is a consequence of a key property of SICs that they form projective 2-designs. This goes some way towards explaining why squared overlap phases play a role. See Ref. 26 for a review of projective t-designs.

Again the restriction to special choices of fiducials can be dropped at the expense of complicating the statement of the theorem a little and significantly complicating the direct proof. In Sec. VII we will formulate a geometrical theorem where this restriction is dropped.

VI. MUTUALLY UNBIASED BASES

The appearance of the parity operator P in Sec. V allows us to give a resolution of the long-standing question of how to relate SICs to mutually unbiased bases (MUB) in prime dimensions. By

definition, a complete set of MUB in dimension p is a collection of $p + 1$ orthonormal bases such that every overlap between vectors in different bases has absolute value squared equal to $1/p$.[15] This definition, like the definition of a SIC, has its origin in quantum state tomography, and MUB have found a number of interesting applications over the years. Complete sets of MUB do exist in all dimensions equal to a power of a prime number,[27] and if the dimension p is a prime number they arise as eigenbases of the $p + 1$ cyclic subgroups of the Weyl–Heisenberg group. (If the dimension is equal to a higher power of a prime number a multipartite Heisenberg group appears. In non-prime power dimensions complete sets of MUB may well not exist, and if they do they are unrelated to the Heisenberg groups.[1,28]) Given this group theoretical connection one expects to find a tight geometrical connection between MUB and SICs in prime dimensional Hilbert spaces. This is indeed so in the very special case of $d = 3$, which was cleared up in 1844.[29] When $d > 3$, it has to be kept in mind that MUB are based on cyclotomic fields, while SICs are two steps beyond that since ray class fields over real quadratic fields come in. Although a loose connection between SICs and MUB in prime dimensions exists,[30] the details have remained elusive.

We can now offer an answer to this question because our Theorem 1 provides us with the means to construct a complete set of MUB in dimension $p = d - 2$ (assumed to be a prime number) from an aligned SIC in dimension $N = d(d - 2)$.[15] In fact, given Wootters' elegant construction of complete sets of MUB in prime dimensions,[31] this result follows trivially from the above, but the details are worth spelling out. The starting point is the observation that in prime dimension the vectors labeling the displacement operators form a true vector space. This is so because the set of integers modulo a prime number form a finite field. This vector space can be regarded as a finite affine plane consisting of p^2 points and $p(p + 1)$ lines containing p points each. The lines are given by the equation

$$j = zi + a, \tag{43}$$

where i, j, and a are integers modulo p while z can also take the formal value ∞, corresponding to a set of "vertical" lines.[30] Thus a line is given by fixing the pair (z, a). Next, consider the p^2 displaced parity operators

$$P_{i,j} = D_{i,j} P D_{-i,-j}. \tag{44}$$

They are renamed as phase point operators, and associated with the p^2 points of the affine plane. We also need operators associated with the $p(p + 1)$ lines of the affine plane. A key fact proved by Wootters is that the operators

$$W^{(z,a)} = \frac{1}{p} \sum_{\text{line}} P_{i,j} \tag{45}$$

are one-dimensional projectors projecting to the vectors in a complete set of MUB. The sum goes over all i, j consistent with Eq. (43) for some given z, a. The construction needs the combinatorics of the affine plane to work, which is certainly available when p is prime.

We now have:

Theorem 3. *If $p = d - 2$ is an odd prime, then a complete set of MUB in dimension p can be obtained by taking affine combinations of projectors to the vectors in an aligned SIC in dimension $d(d - 2)$, and then performing a partial trace.*

Proof. By Theorem 1 and the properties of the partial trace

$$\mathrm{Tr}_d \left(\mathbb{1}_d \otimes D^{(d-2)}_{i,j} \right) |\Psi_{\mathbf{0}}\rangle \langle \Psi_{\mathbf{0}}| \left(\mathbb{1}_d \otimes D^{(d-2)}_{-i,-j} \right) = \frac{1}{d-1} \left(\mathbb{1}_{d-2} + P_{i,j} \right), \tag{46}$$

where we used definition (44) for the displaced parity operators in dimension $d - 2$. The construction uses the $p^2 = (d - 2)^2$ SIC vectors

$$|\Psi_{di,dj}\rangle = \mathbb{1}_d \otimes D^{(d-2)}_{di,j} |\Psi_{\mathbf{0}}\rangle . \tag{47}$$

Using Wootters' formula (45), and the linearity of the trace, we immediately obtain

$$W^{(z,a)} = \mathrm{Tr}_d \left[\frac{d-1}{d-2} \sum_{\text{line}} |\Psi_{di,dj}\rangle\langle\Psi_{di,dj}| - \frac{1}{d}\mathbb{1}_N \right]. \tag{48}$$

By construction, the $(p+1)p$ operators $W^{(z,a)}$ project to the vectors in a complete set of MUB. □

Hence we have a firm relation between MUB in dimension p and SICs in dimension $(p+2)p$. Unfortunately we do not have a way to go from SICs in dimension d to SICs in dimension $d(d-2)$, nor are we close to having this, but if we had, we would have a firm relation between MUB in dimension p and SICs in dimension $p+2$.

VII. THE EMBEDDING OF THE EQUIANGULAR TIGHT FRAMES

We are now ready to prove (for odd d) that the equiangular tight frames observed in Sec. IV have to appear in every aligned SIC. Because the Weyl-Heisenberg group is an operator basis, Schur's lemma implies, for any operator A, that

$$\frac{1}{N}\sum_{\mathbf{p}} D_{\mathbf{p}} A D_{\mathbf{p}}^{\dagger} = \mathbb{1}_N \mathrm{Tr} A. \tag{49}$$

Now suppose the dimension is composite, $N = n_1 n_2$, and assume that the factors are relatively prime and odd. Then Chinese remaindering can be applied, and one can show that

$$\frac{1}{n_1}\sum_{\mathbf{p}_1} (D^{(n_1)}_{\mathbf{p}_1} \otimes \mathbb{1}_{n_2}) A (D^{(n_1)}_{-\mathbf{p}_1} \otimes \mathbb{1}_{n_2}) = \mathbb{1}_{n_1} \otimes \mathrm{Tr}_{n_1} A. \tag{50}$$

We have "isotropized" one factor of the tensor product, and a partial trace appears on the other. A similar equation, with the role of the factors interchanged, will also be used below.

We now specialize to the case $n_1 = d, n_2 = d-2$, and $A = |\Psi_{\mathbf{0}}\rangle\langle\Psi_{\mathbf{0}}|$, where $|\Psi_{\mathbf{0}}\rangle$ is a suitably chosen SIC vector aligned with a SIC vector in dimension d. Then Theorems 1 and 2 give us information about the partial trace that appears on the right hand side. On the other hand, the left hand side has an interesting interpretation. Indeed, we can consider the two operators

$$\begin{aligned} \Pi_1 &\equiv \frac{d-1}{2d}\sum_{i,j=0}^{d-1} |\Psi_{(d-2)i,(d-2)j}\rangle\langle\Psi_{(d-2)i,(d-2)j}| \\ &= \frac{d-1}{2}\frac{1}{d}\sum_{\mathbf{p}_1} (D^{(d)}_{\mathbf{p}_1} \otimes \mathbb{1}_{d-2}) |\Psi_{\mathbf{0}}\rangle\langle\Psi_{\mathbf{0}}| (D^{(d)}_{-\mathbf{p}_1} \otimes \mathbb{1}_{d-2}), \end{aligned} \tag{51}$$

$$\begin{aligned} \Pi_2 &\equiv \frac{d-1}{2(d-2)}\sum_{i,j=0}^{d-3} |\Psi_{di,dj}\rangle\langle\Psi_{di,dj}| \\ &= \frac{d-1}{2}\frac{1}{d-2}\sum_{\mathbf{p}_2} (\mathbb{1}_d \otimes D^{(d-2)}_{\mathbf{p}_2}) |\Psi_{\mathbf{0}}\rangle\langle\Psi_{\mathbf{0}}| (\mathbb{1}_d \otimes D^{(d-2)}_{-\mathbf{p}_2}). \end{aligned} \tag{52}$$

The idea behind the next theorem is that these operators are projectors and can be substituted for the unit operator in the POVM condition (22) provided we restrict ourselves to the subspaces of $\mathbb{C}^N$ to which these operators project.

Theorem 4. *If d is odd, then every aligned SIC in dimension $d(d-2)$ contains two multiplets of smaller equiangular tight frames embedded in it. Each individual SIC vector in an aligned SIC belongs to an equiangular tight frame of d^2 vectors spanning a subspace of dimension $d(d-1)/2$, and another consisting of $(d-2)^2$ vectors spanning a subspace of dimension $(d-1)(d-2)/2$.*

Proof. Combining the definitions (51) and (52), Eq. (50), and Theorems 1 and 2, gives immediately that

$$\Pi_1 = \mathbb{1}_d \otimes \frac{1}{2}(\mathbb{1}_{d-2} + P^{(d-2)}), \tag{53}$$

$$\Pi_2 = \frac{1}{2}(\mathbb{1}_d - P_\theta^{(d)}) \otimes \mathbb{1}_{d-2}. \tag{54}$$

It follows that Π_1 and Π_2 are projectors to subspaces of dimension $d(d-1)/2$ and $(d-1)(d-2)/2$, respectively. To see that the support of Π_1 contains d^2 equiangular SIC vectors, one performs the calculation

$$\begin{aligned} &\langle \Psi_{(d-2)i,(d-2)j} | \Pi_1 | \Psi_{(d-2)i,(d-2)j} \rangle \\ &\quad = \mathrm{Tr} \Pi_1 | \Psi_{(d-2)i,(d-2)j} \rangle \langle \Psi_{(d-2)i,(d-2)j} | = 1, \end{aligned} \tag{55}$$

and similarly for Π_2. The fiducial $|\Psi_{\mathbf{0}}\rangle$ belongs to both subspaces. Conjugating with the Weyl–Heisenberg group, one finds that the subspace defined by the projector Π_1 belongs to an orbit of $(d-2)^2$ subspaces each containing an ETF of type $\left(d(d-1)/2, d^2\right)$, and similarly for Π_2. □

The projectors Π_1 and Π_2, and the Gram matrices of the resulting ETFs, are constructed entirely out of numbers present in the d-dimensional SIC and of suitable roots of unity. Waldron[32] and Goyeneche have already noted that given a SIC in dimension d, one can always construct the Gram matrices corresponding to equiangular tight frames of the types we have here found to be embedded in the aligned $d(d-2)$-dimensional SICs. This result is valid regardless of whether d is odd and even. A version of Theorem 4 that holds for arbitrary d is in fact known, but we postpone its presentation to a companion paper.

In Eq. (25), we also raised the possibility that a regular $(d-1)$-dimensional simplex can be embedded in a $d(d-2)$-dimensional SIC. This happens in three of our examples, namely 8b, 35j, and 120c, and is connected (via our definition of aligned SICs) to the fact that $d-1$ real overlap phases $e^{i\theta_{i,j}}$ occur in the relevant d-dimensional SICs 4a, 7b, and 12b, all of which have an extra anti-unitary symmetry beyond the Zauner symmetry. This is not a property that is inherited on higher rungs of the ladder though; 8b has only 3 real phases and 35j has only 30 real phases.

The embedding of lower dimensional ETFs in the SIC means that non-trivial linear dependencies are present among the vectors of the latter. The general question under what conditions sets of vectors in Weyl–Heisenberg orbits can be linearly dependent has been studied,[33,34] and it is known that linear dependencies do occur, in such orbits, whenever the order of their symmetry group fails to be coprime with the dimension. Some of the linear dependencies that we report here are not covered by these results.

VIII. SYMMETRIES

A striking feature of Tables I and II is that the order of the intrinsic symmetry group of the SICs increases with a factor of two for each rung of the ladder. In fact several of the numerical fiducials in these high dimensions were found because Scott and Grassl[3,4] conjectured the presence of an extra symmetry of order 2 (beyond the order 3 Zauner symmetry), given by the symplectic matrix

$$F_b = \begin{pmatrix} 1-d & 0 \\ 0 & 1-d \end{pmatrix} \in SL(2, \mathbb{Z}_N). \tag{56}$$

In the standard representation that we use[18] an easy calculation gives, after Chinese remaindering according to Eq. (D8), that the corresponding unitary operator is

$$U_b = \mathbb{1} \otimes P, \tag{57}$$

where P is the parity operator in dimension $d-2$. It is easy to prove that this symmetry has to be there.

Theorem 5. *An aligned SIC in an odd dimension is invariant under U_b.*

Proof. Let $|\Psi_0\rangle$ be a strongly centred SIC fiducial. Then Theorem 1 states that the reduced density matrix is

$$\rho_2 = \mathrm{Tr}_1 |\Psi_{\mathbf{0}}\rangle\langle\Psi_{\mathbf{0}}| = \frac{1}{d-1}(\mathbb{1} + P). \tag{58}$$

The Schmidt decomposition[24] of such a state is

$$|\Psi_{\mathbf{0}}\rangle = \sqrt{\frac{2}{d-1}} \sum_{k=1}^{\frac{d-1}{2}} |e_k\rangle\,|f_k\rangle\,. \tag{59}$$

Moreover ρ_2 and $U_b = \mathbb{1} \otimes P$ are diagonal in the Schmidt basis, and U_b manifestly leaves $|\Psi_0\rangle$ invariant. Being a member of the Clifford group it will permute the remaining SIC vectors among themselves. □

A similar argument fails on the left hand factor. The generalized parity operator can be used to construct an operator that leaves $|\Psi_{\mathbf{0}}\rangle$ invariant, but since it is not a member of the Clifford group the last line in the proof fails. This is also the reason why, in Sec. VI, we were able to connect aligned SICs to mutually unbiased bases in dimension $d-2$, but not to MUB in dimension d.

There is more to say about symmetries and dimension towers, and we hope to come back to these issues in a later publication.

IX. CONCLUSIONS

The number theoretical connections between SICs in dimension d and dimension $d(d-2)$ manifest themselves very explicitly in the case of aligned SICs. The number field needed to construct the former is a subfield of that needed to construct the latter.[11,12] Gary McConnell has noted that it can happen that some of the overlap phases in dimension $d(d-2)$ actually belong to the subfield. We have explored a part of this pattern, and it enables us to make significant statements about the Hilbert space geometry of the relevant $d(d-2)$ dimensional SICs. Moreover we have collected evidence, in the form of 19 mostly numerical examples, suggesting that every SIC in dimension d gives rise to a SIC in dimension $d(d-2)$ where this pattern occurs. The higher dimensional member of such a pair is said to be an aligned SIC, and we offered a precise definition of aligned SICs.

In this paper, we concentrated on the case of odd dimensions, in which case there is a canonical tensor product structure. Then the alignment manifests itself as very special entanglement properties (Theorems 1 and 2). If $d-2=p$ is an odd prime number, a complete set of mutually unbiased bases in dimension p can be derived from a higher dimensional SIC (Theorem 3). We also proved that there are non-trivial equiangular tight frames embedded in the $d(d-2)$ dimensional aligned SICs (Theorem 4). This property generalizes to even dimensions, as we will prove in a companion paper. Finally we proved that a conjectured extra symmetry is indeed always present in the aligned SICs (Theorem 5).

We stress that we have only scratched the surface of an intricate pattern. There is more to the story than just squared phases. Then, as we discussed in the Introduction, there are other dimension towers to consider. The field inclusions organize the dimension towers into partially ordered sets with a very intricate structure. Moreover, very recently Grassl and Scott[17] published the results of an investigation of the full sequence (6), corresponding to $D=5$. They conjecture that the ray class SICs in these dimensions have a special symmetry that grows with d, and verify this conjecture by calculating an exact solution for $d=124$ (!) as well as numerical solutions in dimensions 323 and 844 (!) (Further developments have occurred.[37]) Their approach is in a way complementary to ours since we have not focussed on the ray class SICs exclusively. In fact, as Fig. 2 may make clear, the full picture is likely to be even richer than what Fig. 1 begins to suggest.

There is a hope that one can find a way to construct higher dimensional SICs starting from lower dimensional ones, and this hope has served as one of our motivations. There is also an over-riding question: What is the "mechanism" forcing certain algebraic number fields of great independent interest to manifest themselves in the Hilbert space in the precise way they do? We are far from an answer, but we hope our results represent a small step forward.

ACKNOWLEDGMENTS

We thank Gary McConnell for allowing us to use some observations of his as our starting point. We would not have been able to do the work without his support or without the continuous assistance of Andrew Scott (who deserves special thanks for finding the fiducials 195bcd and 120c for us). We also acknowledge Emily King for motivating discussions at a workshop arranged by the Hausdorff Institute and Markus Grassl for spotting several mistakes in an almost final draft. This research was supported in part by the Australian Research Council via EQuS Project No. CE11001013. S.F. acknowledges support from an Australian Research Council Future Fellowship No. FT130101744.

APPENDIX A: ROOTS OF UNITY

When it was first calculated, the SIC in dimension 6 seemed to cement the idea that SICs are significantly more complex than mutually unbiased bases.[35] However, on further reflection, it will be seen that we were not really comparing apples to apples. The exact solutions for the known SICs are written in radicals. If the number $e^{\frac{2\pi i}{n}}$ is written out in radicals, the expression which results is also very complicated (except in special cases). Thus, using the techniques developed by Lagrange, Vandermonde, and Gauss,[13] one finds that the primitive eleventh root of unity is

$$\begin{aligned}\omega_{11} = &-\frac{1}{10} + \left(\frac{1}{40}(-1+b_1) + \frac{1}{20}(1+b_1)b_2\right) b_3 \\ &+ \left(\frac{1}{440}(-1+5b_1) + \frac{1}{220}(-5-b_1)b_2\right) b_3^2 \\ &+ \left(\frac{-1+4b_1}{1210} + \frac{1}{605}(-2-2b_1)b_2\right) b_3^3 \\ &+ \left(\frac{9+5b_1}{133\,10} + \frac{(-45-3b_1)b_2}{133\,10}\right) b_3^4 + \left(\frac{109-25b_1}{585\,640} + \frac{(17+29b_1)b_2}{585\,64}\right) b_3^5 \\ &+ \left(\frac{29+505b_1}{644\,2040} + \frac{(390+37b_1)b_2}{1\,610\,510}\right) b_3^6 + \left(\frac{-1159-1519b_1}{70\,862\,440} + \frac{(49-546b_1)b_2}{17\,715\,610}\right) b_3^7 \\ &+ \left(\frac{-619+7295b_1}{779\,486\,840} + \frac{(2125+2129b_1)b_2}{389\,743\,420}\right) b_3^8 + \left(\frac{26\,459-14\,299b_1}{8\,574\,355\,240} + \frac{(25\,829+10\,629b_1)b_2}{4\,287\,177\,620}\right) b_3^9,\end{aligned} \tag{A1}$$

where

$$\begin{aligned} b_1 &= \sqrt{5}\,, \quad b_2 = \frac{i}{4}\sqrt{10-2b_1}, \\ b_3 &= (\tfrac{1}{4}(561\,671 + 29\,975b_1) + (-24\,365 + 37\,620b_1)b_2)^{\frac{1}{10}}. \end{aligned} \tag{A2}$$

If this formula was used to calculate MUB in dimension 11, the complexity of the resulting expressions would be similar to the complexity of the expressions for the $d = 11$ SICs given by Scott and Grassl.[3] On the other hand, using the transcendental function $f(z) = e^{2\pi iz}$, we find

$$\omega_{11} = f\left(\frac{1}{11}\right). \tag{A3}$$

Hilbert's 12th problem asks for a representation of the numbers needed to construct SICs analogous to the second description of the 11th root of unity. The suggestion is that SICs, if they could be seen through the right number theoretical glasses, are as simple as MUB in prime dimensions are.

APPENDIX B: THE WEYL–HEISENBERG AND CLIFFORD GROUPS

We define the Weyl–Heisenberg group $H(d)$ in dimension d to contain central elements represented by the phase factors[18]

$$\tau = -e^{\frac{i\pi}{d}}, \quad \omega = \tau^2 = e^{\frac{2\pi i}{d}}. \tag{B1}$$

(Multiplication with the unit matrix is left understood whenever this cannot cause confusion.) If the dimension d is odd, as we assume, then $(d+1)/2$ is an integer and there holds

$$\omega^{\frac{d+1}{2}} = \left(e^{\frac{\pi i}{d}}\right)^{d+1} = \tau. \tag{B2}$$

Both τ and ω are dth roots of unity in this case. If d is even some complications arise, and we postpone this case to a separate paper. Here we only wish to note the fact, evident from the introduction, that odd and even d show some differences also at the level of algebraic number theory.

The remaining group elements are given by d^2 displacement operators which we write interchangeably as $D_{i,j}$ and $D_{\mathbf{p}}$, with the understanding that $\mathbf{p}$ is a two-component "vector" with components i, j that are integers modulo d. The displacement operators obey $D_{\mathbf{p}}^{\dagger} = D_{-\mathbf{p}}$ and

$$D_{\mathbf{p}} D_{\mathbf{q}} = \tau^{\langle \mathbf{p},\mathbf{q}\rangle} D_{\mathbf{p}+\mathbf{q}} = \omega^{\langle \mathbf{p},\mathbf{q}\rangle} D_{\mathbf{q}} D_{\mathbf{p}}, \tag{B3}$$

where the exponent is given in terms of the components of the "vectors,"

$$\mathbf{p} = \begin{pmatrix} i \\ j \end{pmatrix}, \quad \mathbf{q} = \begin{pmatrix} k \\ l \end{pmatrix} \quad \Rightarrow \quad \langle \mathbf{p}, \mathbf{q} \rangle = kj - li. \tag{B4}$$

Thus $\langle\ ,\ \rangle$ is a symplectic form. An explicit matrix representation is

$$(D_{i,j})_{r,s} = \tau^{ij+2js} \delta_{r,s+i}. \tag{B5}$$

This representation is essentially unique, once $D_{0,\,j}$ is chosen to be diagonal.

Frequently we will have displacement operators for dimensions d and $d(d-2)$ occurring in the same formula. When necessary to avoid confusion, operators are supplied with superscripts denoting the dimension in which they act, e.g., $D_{\mathbf{p}}^{(d)}, D_{\mathbf{p}}^{(d-2)}, D_{\mathbf{p}}^{(N)}$. In this appendix no superscripts are necessary because the dimension is always an arbitrary integer d. Occasionally we use subscripts for the same purpose; thus, ω_d is the dth root of unity whenever this is not obvious.

If F is a $GL(2, \mathbb{Z}_d)$ matrix, that is to say a 2×2 matrix with entries that are integers modulo d, then we find when we calculate in modulo d arithmetic that

$$\langle F\mathbf{p}, F\mathbf{q} \rangle = \langle \mathbf{p}, \mathbf{q} \rangle \det F. \tag{B6}$$

The condition $\det F = 1$ defines the symplectic subgroup $SL(2, \mathbb{Z}_d)$. This group is part of the unitary automorphism group of the Weyl–Heisenberg group, also known as the Clifford group. Every matrix $F \in SL(2, \mathbb{Z}_d)$ is represented by a unitary matrix U_F. By definition, a Zauner operator is associated to a matrix of order three and trace equal to -1. The matrices F_z and F_a, corresponding, respectively, to the "universal" Zauner operator and to the "unusual" Zauner operator in dimensions of the form $d = 9k + 3$, are

$$F_z = \begin{pmatrix} 0 & d-1 \\ 1 & -1 \end{pmatrix}, \quad F_a = \begin{pmatrix} 1 & 3 \\ 3k & d-2 \end{pmatrix}. \tag{B7}$$

See Refs. 3 and 5 for more. Matrices with $\det F = -1$ are represented as anti-unitary operators and as such belong to the extended Clifford group.[18]

APPENDIX C: PARITY OPERATORS

The symplectic group contains a special involution of order 2, whose unitary representative is known as the parity operator,

$$F = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \Rightarrow \quad U_F \equiv P. \tag{C1}$$

If d is odd, this is a unitary Hermitian operator with spectrum $[(d+1)/2, (d-1)/2]$. When d is odd, the integer 2 has a multiplicative inverse 2^{-1} in arithmetic modulo d, and we can calculate that

$$\mathrm{Tr} D_{\mathbf{p}} P = \mathrm{Tr} P D_{2^{-1}\mathbf{p}} P^2 D_{2^{-1}\mathbf{p}} P = \mathrm{Tr} D_{2^{-1}\mathbf{p}} P D_{-2^{-1}\mathbf{p}} = \mathrm{Tr} P = 1. \tag{C2}$$

Hence the parity operator can be expanded as

$$P = \frac{1}{d} \sum_{\mathbf{p}} D_{-\mathbf{p}}. \tag{C3}$$

Conjugating with the Weyl-Heisenberg group, we obtain d^2 parity operators belonging to the Clifford group. They are the displaced parity operators used in Sec. VI and were called phase point operators by Wootters.[31]

It is a property of SIC overlap phases that the generalized parity operator P_θ occurring in Eq. (42) is isospectral with the parity operator P[25] but P_θ does not belong to the Clifford group.

APPENDIX D: THE CHINESE REMAINDER THEOREM

We are interested in dimensions of the form $N = d(d-2)$. When N is odd d and $d-2$ are relatively prime integers. A theorem from elementary number theory then comes into play: the Chinese remainder theorem states that if n_1 and n_2 are relatively prime, then any integer r modulo $N = n_1 n_2$ can be uniquely expressed in terms of a pair of integers $r_i = r \bmod n_i$ as

$$r = r_1 n_2 n_2^{-1} + r_2 n_1 n_1^{-1}. \tag{D1}$$

Throughout, $n_2^{-1}(n_1^{-1})$ denotes the inverse of the integer $n_2(n_1)$ in arithmetic modulo $n_1(n_2)$. The formula expresses a ring isomorphism between $\mathbb{Z}_N$, the ring of integers modulo N, and the ring $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. This was appreciated in ancient China because it allows arithmetic modulo a large integer N to be carried out modulo the smaller integers n_1 and n_2, and the end result reconverted to an integer modulo N. The application to Weyl–Heisenberg groups as an approach to the SIC problem was pioneered by David Gross.[36]

The Chinese remainder theorem can be used to express the isomorphism between the corresponding cyclic groups and also the isomorphism $H(N) = H(n_1) \times H(n_2)$. We use $\omega = e^{\frac{2\pi i}{N}}$ to represent $H(N)$. There holds

$$\omega = \omega_{n_1}^{n_2^{-1}}\, \omega_{n_2}^{n_1^{-1}}. \tag{D2}$$

Namely

$$e^{\frac{2\pi i}{N}} = e^{\frac{2\pi i}{n_1 n_2}\cdot 1} = e^{\frac{2\pi i}{n_1 n_2}(n_2 n_2^{-1} + n_1 n_1^{-1})} = e^{\frac{2\pi i}{n_1} n_2^{-1}}\, e^{\frac{2\pi i}{n_2} n_1^{-1}}. \tag{D3}$$

Given that ω_1 is a primitive root of unity, so is $\omega_1^{n_2^{-1}}$, so it would be possible to use this to represent $H(n_1)$. However, we choose not to. We then find that

$$D_{i,j} = D^{(n_1)}_{i_1, n_2^{-1} j_1} \otimes D^{(n_2)}_{i_2, n_1^{-1} j_2}, \tag{D4}$$

where the matrix representation is, say,

$$D^{(n_1)}_{i_1, n_2^{-1} j_1} = \omega_1^{(2n_2)^{-1} i_i j_i + n_2^{-1} j_1 s_1}\, \delta_{r_1, s_1 + i_1}. \tag{D5}$$

The subscripts on the indices are superfluous since the arithmetic used for the indices is automatically modulo n_1. Using the vector notation, we write

$$D_{\mathbf{p}} = D^{(n_1)}_{H_1 \mathbf{p}} \otimes D^{(n_2)}_{H_2 \mathbf{p}}, \tag{D6}$$

where

$$H_1 = \begin{pmatrix} 1 & 0 \\ 0 & n_2^{-1} \end{pmatrix}, \quad H_2 = \begin{pmatrix} 1 & 0 \\ 0 & n_1^{-1} \end{pmatrix}. \tag{D7}$$

The Clifford group also splits into a direct product. One finds

$$U_F = U^{(n_1)}_{F_1} \otimes U^{(n_2)}_{F_2} = U^{(n_1)}_{H_1 F H_1^{-1}} \otimes U^{(n_2)}_{H_2 F H_2^{-1}}. \tag{D8}$$

Now we specialize to $n_1 = d$ and $n_2 = d-2$. Then

$$n_2^{-1} \bmod n_1 \; = n_1^{-1} \bmod n_2 = \frac{d-1}{2} \equiv \kappa, \tag{D9}$$

where the integer κ was defined in the last step. [Proof: Calculating modulo $d-2$, we find $d(d-1)/2 = 2(d-1)/2 = d - 1 = 1$. The point is that $(d-1)/2$ is an ordinary integer. *Mutatis mutandis* when calculating modulo d.] Thus

$$H \equiv H_1 = H_2 = \begin{pmatrix} 1 & 0 \\ 0 & \kappa \end{pmatrix}. \tag{D10}$$

For the symplectic matrices, one finds

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \Rightarrow \quad HFH^{-1} = \begin{pmatrix} \alpha & \kappa^{-1}\beta \\ \kappa\gamma & \delta \end{pmatrix}, \tag{D11}$$

where we decide on the modulus in the last step.

In conclusion, in dimensions $N = d(d-2)$ with d odd, the Weyl–Heisenberg group allows us to express the Hilbert space as $\mathbb{C}^N = \mathbb{C}^d \otimes \mathbb{C}^{d-2}$ in a preferred way.

[1] G. Zauner, "Quantendesigns. Grundzüge einer nichtkommutativen designtheorie," Ph.D. thesis, University of Wien, 1999; Quantum designs: Foundations of a noncommutative design theory," Int. J. Quantum Inf. **9**, 445 (2011).
[2] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, "Symmetric informationally complete quantum measurements," J. Math. Phys. **45**, 2171 (2004).
[3] A. J. Scott and M. Grassl, "SIC-POVMs: A new computer study," J. Math. Phys. **51**, 042203 (2010).
[4] A. J. Scott, "SICs: Extending the list of solutions," e-print arXiv:1703.03993.
[5] M. Appleby, T.-Y. Chien, S. Flammia, and S. Waldron, "Constructing exact symmetric informationally complete measurements from numerical solutions," e-print arXiv:1703.05981.
[6] C. A. Fuchs, M. C. Hoang, and B. C. Stacey, "The SIC question: History and state of play," Axioms **6**, 21 (2017).
[7] H. Weyl, *Theory of Groups and Quantum Mechanics* (Dutton, New York, 1932).
[8] S. D. Howard, A. R. Calderbank, and W. Moran, "The finite Heisenberg–Weyl group in radar and communications," EURASIP J. Adv. Signal Process. **2006**, 85865.
[9] Y. I. Manin, "Real multiplication and noncommutative geometry (ein Alterstraum)," in *The Legacy of Niels Henrik Abel*, edited by O. A. Laudal and R. Piene (Springer, 2004).
[10] D. M. Appleby, H. Yadsan-Appleby, and G. Zauner, "Galois automorphisms of symmetric measurements," Quantum Inf. Comput. **13**, 672 (2013).
[11] M. Appleby, S. Flammia, G. McConnell, and J. Yard, "Generating ray class fields of real quadratic fields via complex equiangular lines," e-print arXiv:1604.06098.
[12] M. Appleby, S. Flammia, G. McConnell, and J. Yard, "SICs and algebraic number theory," Found. Phys. **47**, 1 (2017).
[13] J.-P. Tignol, *Galois Theory of Algebraic Equations* (World Scientific, Singapore, 2001).
[14] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields. With Two Appendices by Olga Taussky* (Springer, 1978).
[15] I. D. Ivanović, "Geometrical description of state determination," J. Phys. A: Math. Gen. **14**, 3241 (1981).
[16] N. Schappacher, *On the History of Hilbert's 12th Problem. A Comedy of Errors, Matériaux Pour l'historie des Mathématiques au XXe Siècle* (Nice, 1996), p. 243, Séminaires et Congres 3, Paris, 1998.
[17] M. Grassl and A. J. Scott, "Fibonacci–Lucas SIC-POVMs," J. Math. Phys. (unpublished); e-print arXiv:1707.02944.
[18] D. M. Appleby, "SIC-POVMs and the extended Clifford group," J. Math. Phys. **46**, 052107 (2005).
[19] H. Zhu, "SIC-POVMs and Clifford groups in prime dimensions," J. Phys. A: Math. Theor. **43**, 305305 (2010).
[20] H. Zhu, "Super-symmetric informationally complete measurements," Ann. Phys. **362**, 311 (2015).
[21] J. Schwinger, "Unitary operator bases," Proc. Natl. Acad. Sci. U. S. A. **46**, 570 (1960).
[22] J. J. Benedetto and M. Fickus, "Finite normalized tight frames," Adv. Comput. Math. **18**, 357 (2003).
[23] M. Fickus and D. G. Mixon, "Tables of the existence of equiangular tight frames," e-print arXiv:1504.00253.
[24] A. Ekert and P. L. Knight, "Entangled quantum systems and the Schmidt decomposition," Am. J. Phys. **63**, 415 (1995).
[25] D. Goyeneche, M. Appleby, I. Bengtsson, and S. Flammia (unpublished).
[26] A. Belovs, "Welch bounds and quantum state tomography," M.S. thesis, University of Waterloo, 2008.
[27] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," Ann. Phys. **191**, 363 (1989).
[28] M. Aschbacher, A. M. Childs, and P. Wocjan, "The limitations of nice mutually unbiased bases," J. Algebr. Comb. **25**, 111 (2007).
[29] O. Hesse, "Über die wendepuncte der curven dritter ordnung," J. Reine Angew. Math. **28**, 97 (1844).
[30] D. M. Appleby, H. B. Dang, and C. A. Fuchs, "Symmetric informationally-complete quantum states as analogues to orthonormal bases and minimum uncertainty states," Entropy **16**, 1484 (2014).
[31] W. K. Wootters, "A Wigner-function formulation of finite-state quantum mechanics," Ann. Phys. **176**, 1 (1987).
[32] S. Waldron, "A sharpening of the Welch bounds and the existence of real and complex spherical t–design," IEEE Trans. Inf. Theory **63**, 6849 (2017).
[33] H. B. Dang, K. Blanchfield, I. Bengtsson, and D. M. Appleby, "Linear dependencies in Weyl–Heisenberg orbits," Quant. Inf. Proc. **12**, 3449 (2013).
[34] R.-D. Malikiosis, "Spark deficient Gabor frames," e-print arXiv:1602.09012.
[35] M. Grassl, "On SIC-POVMs and MUBs in dimension 6," e-print arXiv:quant-ph/0406175.
[36] D. M. Appleby, I. Bengtsson, S. Brierley, M. Grassl, D. Gross, and J.-Å. Larsson, "The monomial representations of the Clifford group," Quantum Inf. Comput. **12**, 0404 (2012).
[37] Note added in proof: After this paper was completed Grassl and Scott posted a revised version of Ref. 17 in which they provide an exact solution for dimension 323 (!!). The results we report were of some assistance in calculating this solution.

Paper II

Aligned SICs and embedded tight frames in even dimensions

OPEN ACCESS
IOP Publishing
Journal of Physics A: Mathematical and Theoretical
J. Phys. A: Math. Theor. **52** (2019) 425302 (25pp)
https://doi.org/10.1088/1751-8121/ab434e

Aligned SICs and embedded tight frames in even dimensions

Ole Andersson and Irina Dumitru

Department of Physics, Stockholm University, 106 91 Stockholm, Sweden

E-mail: ole.andersson@fysik.su.se and irina.dumitru@fysik.su.se

Received 1 June 2019, revised 12 August 2019
Accepted for publication 10 September 2019
Published 24 September 2019

Abstract

Alignment is a geometric relation between pairs of Weyl–Heisenberg SICs, one in dimension d and another in dimension $d(d-2)$, manifesting a well-founded conjecture about a number-theoretical connection between the SICs. In this paper, we prove that if d is even, the SIC in dimension $d(d-2)$ of an aligned pair can be partitioned into $(d-2)^2$ tight d^2-frames of rank $d(d-1)/2$ and, alternatively, into d^2 tight $(d-2)^2$-frames of rank $(d-1)(d-2)/2$. The corresponding result for odd d is already known, but the proof for odd d relies on results which are not available for even d. We develop methods that allow us to overcome this issue. In addition, we provide a relatively detailed study of parity operators in the Clifford group, emphasizing differences in the theory of parity operators in even and odd dimensions and discussing consequences due to such differences. In a final section, we study implications of alignment for the symmetry of the SIC.

Keywords: SIC-POVM, frame theory, Weyl–Heisenberg group, symmetry, parity operator, Chinese remainder

1. Introduction

An informationally complete POVM is one that can be used to reconstruct any quantum state, pure or mixed. Since an n-dimensional state is given by an $n \times n$ unit-trace Hermitian matrix, and, hence, by $n^2 - 1$ real parameters, a minimal informationally complete POVM has to consist of n^2 unit rank elements, giving $n^2 - 1$ independent measurement results. This paper deals with such POVMs. Specifically, it deals with so-called symmetric informationally complete POVMs [1] (SIC-POVMs, or SICs, for short). SICs are exceptional among informationally complete POVMs in the sense that the information overlap of the measurement results is

minimal, making them optimal candidates for state tomography [2]. These remarkable tomographic properties reflect that the SIC elements constitute an equiangular tight frame of maximally many vectors.

Whether SICs exist in all dimensions is still an open question. In his doctoral thesis [3], Zauner conjectured that in all finite dimensions at least one SIC exists that is covariant under the discrete Weyl–Heisenberg group, and he further conjectured that at least one such SIC has an order 3 unitary symmetry. These conjectures have been guiding the search for SIC-POVMs ever since. As a result of such searches, we are now confident that we know all Weyl–Heisenberg covariant SICs in Hilbert spaces up to dimension 50 [4], and, interestingly, all of them have the symmetry conjectured by Zauner. Furthermore, at least one SIC has been found in each dimension up to 181 [5], and there are several known SICs in dimensions above that, with the highest dimension being 2208 [5].

In this paper, we are interested in properties of Weyl–Heisenberg SIC-POVMs. In particular, we are interested in properties of what we call *aligned* SICs in composite dimensions of the form $d(d-2)$. Alignment is a geometric relation between a SIC in dimension $d(d-2)$ and a SIC in the corresponding dimension d which manifests a conjectured number-theoretical connection between SICs in such dimensions [6]. The presence of alignment was discovered numerically [7] by looking at all SICs known at the time in dimensions d and $d(d-2)$, the highest value of d being 15. For each SIC in dimension d, a SIC in dimension $d(d-2)$ was found to which it is aligned. In the meantime, the observation of this relation guided the search for a SIC in dimension $323 = 19(19-2)$ [8]. All known aligned SICs in composite dimension $d(d-2)$ have also been observed to exhibit a remarkable geometric property of their own, namely the embedding of lower-dimensional equiangular tight frames [7, 9, 10].

In dimensions being the product of two relatively prime factors, each representation of the Weyl–Heisenberg group splits into a tensor product representation. This result was proven in [11] using the Chinese remainder theorem and application of this result is, nowadays, referred to as *Chinese remaindering*. Chinese remaindering can be applied in odd dimensions of the form we are interested in, since for odd d the factors d and $d-2$ are relatively prime, and has indeed been used to prove the existence of embedded tight frames in the SIC in the larger dimension of an aligned pair [7]. However, for even d, Chinese remaindering cannot be applied, at least not immediately. In the current paper, we use special properties of representations of the Weyl–Heisenberg group in dimensions divisible by 4 to overcome this issue (and thereby lay out an approach for the treatment of more general composite dimensions whose factors have 2 as the greatest common divisor), and we extend the results in [7] to even dimensions of the form $d(d-2)$.

Parity operators in the Clifford group play a role in our treatment of aligned SICs, and they too show different behaviors in even and odd dimensions. The differences are similar to those that give rise to a uniqueness issue in the extension of the Wigner function to discrete spaces: The Wigner function can be defined using parity operators [12], which allows for an extension to discrete spaces. The extension is canonical in the odd-dimensional case [13], but it is not so in the even-dimensional case [14, 15].

The paper is structured as follows. Section 2 deals with the theory of SIC-POVMs and equiangular tight frames and introduces the notion of alignment. In section 3 we use the apparatus of Chinese remaindering to prove the existence of equiangular tight frames embedded in aligned SICs. Part of this section is dedicated to a discussion of parity operators. Section 4 explores the consequences of alignment for the symmetry of SICs.

2. Equiangular tight frames and aligned SICs

An equiangular tight m-frame in an n-dimensional Hilbert space is a set of unit-length vectors $|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{m-1}\rangle$ which satisfies the two conditions

$$|\langle\psi_a|\psi_b\rangle|^2 = \frac{m-n}{n(m-1)} \text{ if } a \neq b, \tag{1}$$

$$\frac{n}{m}\sum_{a=0}^{m-1} |\psi_a\rangle\langle\psi_a| = \mathbb{1}. \tag{2}$$

That the common angle between any two vectors in the frame has to be the one specified in (1) follows from the assumption that the frame is normalized and the tightness condition (2). Furthermore, one can show that such a frame can contain neither less than n nor more than n^2 vectors, see [16]. In the extremal case $m = n$, an equiangular tight m-frame is the same thing as an orthonormal basis, and if $m = n^2$, an equiangular tight m-frame is a SIC. The acronym SIC is a short version of the longer SIC-POVM which stands for 'symmetric informationally complete positive-operator valued measure'. As was mentioned in the introduction, such measures have exceptional tomographic properties. Here, however, we will only be concerned with their geometric characteristics. For the reader's convenience we repeat the defining conditions satisfied by a SIC:

$$|\langle\psi_a|\psi_b\rangle|^2 = \frac{1}{n+1} \text{ if } a \neq b, \qquad \frac{1}{n}\sum_{a=0}^{n^2-1} |\psi_a\rangle\langle\psi_a| = \mathbb{1}. \tag{3}$$

2.1. Weyl–Heisenberg SICs and alignment

Zauner formulated a very strong conjecture in his thesis [3], namely that in every dimension a SIC exists which is an orbit under a unitary representation of the discrete Weyl–Heisenberg group. He also conjectured that in every dimension a SIC fiducial vector can be chosen among the eigenvectors of an operator of order 3 in the Clifford group, nowadays referred to as a 'Zauner operator'. A SIC fiducial vector is a unit length vector which generates a SIC when the unitaries in the Weyl–Heisenberg group displace it, and the Clifford group is the normalizer of the Weyl–Heisenberg group, see section 2.1.3. Almost all known examples of SICs are generated by irreducible representations of the Weyl–Heisenberg group [4, 17], and in this paper we will only consider such SICs. We call them Weyl–Heisenberg SICs or WH-SICs for short.

2.1.1. The Weyl–Heisenberg group. The discrete Weyl–Heisenberg group $\mathrm{WH}(n)$ has three generators ω, X, and Z. The generators have order n, ω commutes with all the group elements, and the other two generators satisfy the commutation relation $ZX = \omega XZ$.

Let (ω_n, X_n, Z_n) be an irreducible unitary representation of $\mathrm{WH}(n)$ on an n-dimensional Hilbert space (i.e. ω_n, X_n, and Z_n are the unitary operators corresponding to ω, X, and Z). Then, by a theorem of Weyl [18, chapter IV, section 15], ω_n is a multiple of the identity operator, and X_n and Z_n are represented by generalized Pauli matrices relative to an orthonormal basis $\{|u\rangle : u \in \mathbb{Z}_n\}$:

$$X_n = \sum_{u=0}^{n-1} |u+1\rangle\langle u|, \qquad Z_n = \sum_{u=0}^{n-1} \omega_n^u |u\rangle\langle u|. \tag{4}$$

The multiplier of the identity in ω_n (which we also denote by ω_n) can be any primitive nth root of unity. In this paper, however, we will only consider representations of $\mathrm{WH}(n)$ in which $\omega_n = \mathrm{e}^{2\pi\mathrm{i}/n}$.

2.1.2. Displacement operators. It is convenient for many purposes, including our own, to define so-called displacement operators. We thus set $\tau_n = -\mathrm{e}^{\pi\mathrm{i}/n}$ and, for any pair of integers a and b, define

$$D_{a,b}^{(n)} = \tau_n^{ab} X_n^a Z_n^b. \tag{5}$$

(The superscript '(n)' is to indicate that the displacement operator acts on an n-dimensional Hilbert space.) In odd dimensions τ_n is a power of ω_n. Hence the displacement operators all belong to and generate the representation of the Weyl–Heisenberg group. In even dimensions, however, this is not the case, and the group generated by the displacement operators is larger than the representation of the Weyl–Heisenberg group. The 'double-dimensional' order of τ_n complicates matters. Still, there are reasons, see [19], for defining the displacement operators as in (5) in all dimensions. In any case, the displacement operators generate the same SIC as the Weyl–Heisenberg group when fed with the same SIC fiducial vector.

A straightforward calculation shows that

$$D_{a,b}^{(n)} D_{k,l}^{(n)} = \tau_n^{bk-al} D_{a+k,b+l}^{(n)}. \tag{6}$$

From this follows that the Hermitian conjugate of $D_{a,b}^{(n)}$ is $D_{-a,-b}^{(n)}$ and that the displacement operators satisfy the commutation rule

$$D_{a,b}^{(n)} D_{k,l}^{(n)} = \omega_n^{bk-al} D_{k,l}^{(n)} D_{a,b}^{(n)}. \tag{7}$$

The displacement operators also satisfy the translation properties

$$D_{a+n,b}^{(n)} = (-1)^{(n+1)b} D_{a,b}^{(n)}, \qquad D_{a,b+n}^{(n)} = (-1)^{(n+1)a} D_{a,b}^{(n)}. \tag{8}$$

Thus, they are periodic in the indices if n is odd, while they are periodic or anti-periodic depending on the parity of the index being translated if n is even.

We will frequently use the fact that the displacement operators (or their Hermitian conjugates) corresponding to indices $0 \leqslant a, b \leqslant n-1$ form an orthogonal operator basis. The inner product of two displacement operators in the basis is $\mathrm{tr}\big(D_{-a,-b}^{(n)} D_{k,l}^{(n)}\big) = n\delta_{ak}\delta_{bl}$ and, hence, any operator A can be expanded as

$$A = \frac{1}{n} \sum_{a,b=0}^{n-1} \mathrm{tr}(D_{-a,-b}^{(n)} A) D_{a,b}^{(n)} = \frac{1}{n} \sum_{a,b=0}^{n-1} \mathrm{tr}(D_{a,b}^{(n)} A) D_{-a,-b}^{(n)}. \tag{9}$$

This is *the expansion of A in the displacement operator basis*.

2.1.3. The Clifford group. The Clifford group is the normalizer of the Weyl–Heisenberg group in the unitary group. In other words, the Clifford group consists of those unitary operators V which are such that $VX_nV^\dagger$ and $VZ_nV^\dagger$ belong to the representation of the Weyl–Heisenberg group. This definition also determines the Clifford group as an abstract group: By the theorem of Weyl referred to in section 2.1.1, any two irreducible representations of the Weyl–Heisenberg

group (which assign the same value to ω) are canonically unitarily invariant. Hence, so are the Clifford groups associated with the different representations. We refer to [19] for an extensive account of the relation between the Clifford group and SICs.

Let $\bar{n} = n$ if n is odd and $\bar{n} = 2n$ if n is even. The symplectic group $\mathrm{SL}(2, \mathbb{Z}_{\bar{n}})$, i.e. the group of 2×2 matrices with entries in the ring of integers modulo $\bar{n}$ and determinant 1, admits a projective representation $F \to V_F$ in the Clifford group, see [19]. If

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{10}$$

is a symplectic matrix for which β is invertible modulo $\bar{n}$, then, in the basis relative to which X_n and Z_n are represented by generalized Pauli matrices (4),

$$V_F = \frac{1}{\sqrt{n}} \sum_{u,v=0}^{n-1} \tau_n^{\beta^{-1}(\alpha v^2 - 2uv + \delta u^2)} |u\rangle\langle v|. \tag{11}$$

We use the language in [19] and call symplectic matrices with β invertible modulo $\bar{n}$ *prime*. For non-prime F one can always find prime symplectic matrices F_1 and F_2 such that $F = F_1 F_2$, see [19]. We then define

$$V_F = V_{F_1} V_{F_2}. \tag{12}$$

The definition (12) together with (11) determines V_F up to a phase, meaning that different prime decompositions of F give rise to operators V_F which may differ by a phase factor. This indeterminacy is what is meant by the representation being 'projective'. Henceforth, we refer to unitary operators of the form V_F as symplectic unitaries. The symplectic unitaries satisfy the important identity

$$V_F D^{(n)}_{a,b} V_F^\dagger = D^{(n)}_{F(a,b)}. \tag{13}$$

The indices of the displacement operator in the right-hand side are the entries of the matrix obtained by applying F to $(a, b)^T$.

2.2. Alignment

Let $|\psi_{a,b}\rangle$ be the vector obtained by applying $D^{(n)}_{a,b}$ to a SIC fiducial vector $|\psi_{0,0}\rangle$. Unless $a = b = 0 \bmod n$, the magnitude of the overlap between $|\psi_{a,b}\rangle$ and $|\psi_{0,0}\rangle$ is $1/\sqrt{n+1}$. We define the overlap phases for a WH-SIC in dimension n by

$$\mathrm{e}^{\mathrm{i}\theta^{(n)}_{a,b}} = \begin{cases} 1 & \text{if } a = b = 0 \bmod n, \\ \sqrt{n+1}\langle\psi_{0,0}|\psi_{a,b}\rangle & \text{otherwise.} \end{cases} \tag{14}$$

Alignment is a geometric relation between WH-SICs in dimensions d and $n = d(d-2)$ which manifests a conjectured number-theoretical connection between the overlap phases of WH-SICs in dimensions d and $d(d-2)$: We say that a WH-SIC in dimensions d is aligned with a WH-SIC in dimension $n = d(d-2)$ if there exist choices of fiducial vectors for these such that if $a \neq 0 \bmod (d-2)$ or $b \neq 0 \bmod (d-2)$, then

$$\mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} = \begin{cases} 1 & \text{if } d \text{ is odd,} \\ -(-1)^{(a+1)(b+1)} & \text{if } d \text{ is even,} \end{cases} \tag{15}$$

and if $a \neq 0 \bmod d$ or $b \neq 0 \bmod d$, then

$$\mathrm{e}^{\mathrm{i}\theta^{(n)}_{(d-2)a,(d-2)b}} = \begin{cases} -\mathrm{e}^{2\mathrm{i}\theta^{(d)}_{\alpha a+\beta b,\gamma a+\delta b}} & \text{if } d \text{ is odd,} \\ (-1)^{(a+1)(b+1)}\mathrm{e}^{2\mathrm{i}\theta^{(d)}_{\alpha a+\beta b,\gamma a+\delta b}} & \text{if } d \text{ is even,} \end{cases} \tag{16}$$

where α, β, γ, and δ are integers modulo d such that $\alpha\delta - \beta\gamma = \pm 1$. McConnell was the first to observe these relations for the phases [20]. The concept of alignment was introduced in [7], and, supported by extensive numerical and analytical evidence, the authors conjectured that aligned pairs of SICs exist for all values of d. It was also proven in [7] that if d is odd, any SIC in dimension $d(d-2)$ which satisfies (15) can be partitioned into $(d-2)^2$ equiangular tight d^2-frames of rank $d(d-1)/2$, or, alternatively, into d^2 equiangular tight $(d-2)^2$-frames of rank $(d-1)(d-2)/2$. Below we prove that the same is true if d is even.

Whether one of the conditions (15) and (16) follows from the other is not known. But no SIC is known which satisfies only one of the conditions. The results in this paper, however, only rely on (15) being fulfilled. When we use the expression 'aligned SIC' we refer to the higher-dimensional member of an aligned pair.

2.3. Unitary equivalence

Alignment is a property shared among unitarily equivalent WH-SICs. Therefore, when examining those intrinsic properties of WH-SICs which are consequences of alignment, one may first apply any suitable unitary to the vectors of the SIC and then proceed with the study. The theorem of Weyl referred to in section 2.1.1 allows one to do this at the level of representations. For according to that theorem, two irreducible n-dimensional representations of $\mathrm{WH}(n)$ which assign the same multiple of the unit operator to ω are unitarily equivalent. We will use this freedom to rotate the representation when convenient.

3. Equiangular tight frames in aligned SICs

Suppose that $\{|\psi_{a,b}\rangle\}$ is an aligned WH-SIC in dimension $n = d(d-2)$. We prove that if n is even, the d^2-frame

$$\{|\psi_{(d-2)a,(d-2)b}\rangle : a, b = 0 \ldots d-1\} \tag{17}$$

spans and is tight in a $d(d-1)/2$-dimensional space, and the $(d-2)^2$-frame

$$\{|\psi_{da,db}\rangle : a, b = 0 \ldots d-3\} \tag{18}$$

spans and is tight in a $(d-1)(d-2)/2$-dimensional space. By shifting the frame in (17), respectively (18), by appropriate displacement operators the SIC gets partitioned into $(d-2)^2$ equiangular tight d^2-frames, respectively into d^2 equiangular tight $(d-2)^2$-frames. The corresponding result for odd n was proven in [7]. Notice that, since the equiangularity condition (1) is automatically satisfied, it suffices to prove that

$$\Pi_1 = \frac{d-1}{2d}\sum_{a,b=0}^{d-1} |\psi_{(d-2)a,(d-2)b}\rangle\langle\psi_{(d-2)a,(d-2)b}|, \tag{19}$$

$$\Pi_2 = \frac{d-1}{2(d-2)}\sum_{a,b=0}^{d-3} |\psi_{da,db}\rangle\langle\psi_{da,db}|, \tag{20}$$

are projection operators of rank $d(d-1)/2$ and $(d-1)(d-2)/2$, respectively.

3.1. Block-diagonal splitting

When n is even, d and $(d-2)$ also have to be even. We write $d = 2n_1$ and $(d-2) = 2n_2$. The integers n_1 and n_2 are relatively prime, being consecutive integers. In appendix A it is shown that, due to this fact, the Hilbert space can be decomposed into four (n_1n_2)-dimensional subspaces, and that there are irreducible representations of $\mathrm{WH}(n_1n_2)$ on these subspaces such that the displacement operators with even indices are block-diagonal:

$$D^{(n)}_{2a,2b} = (-1)^{ab} \begin{pmatrix} D^{(n_1n_2)}_{a,b} & & & \\ & \omega^{a}_{2n_1n_2} D^{(n_1n_2)}_{a,b} & & \\ & & \omega^{b}_{2n_1n_2} D^{(n_1n_2)}_{a,b} & \\ & & & \omega^{a+b}_{2n_1n_2} D^{(n_1n_2)}_{a,b} \end{pmatrix}. \tag{21}$$

Furthermore, Chinese remaindering, see appendix B, introduces a tensor product in each subspace which splits it into an n_1-dimensional factor and an n_2-dimensional factor. The subspace displacement operators then split according to

$$D^{(n_1n_2)}_{a,b} = D^{(n_1)}_{a,\kappa_2 b} \otimes D^{(n_2)}_{a,\kappa_1 b}. \tag{22}$$

The integers κ_1 and κ_2 are the multiplicative inverses of n_1 and n_2 modulo $\bar{n}_2$ and $\bar{n}_1$, respectively. (See appendix B.) We have in particular that

$$(-1)^{n_1^2 ab} D^{(n_1n_2)}_{n_1a,n_1b} = D^{(n_1)}_{n_1a,\kappa_2 n_1 b} \otimes (-1)^{n_1^2 ab} D^{(n_2)}_{n_1a,\kappa_1 n_1 b} = \mathbb{1}_{n_1} \otimes D^{(n_2)}_{a,b}, \tag{23}$$

$$(-1)^{n_2^2 ab} D^{(n_1n_2)}_{n_2a,n_2b} = (-1)^{n_2^2 ab} D^{(n_1)}_{n_2a,\kappa_2 n_2 b} \otimes D^{(n_2)}_{n_2a,\kappa_1 n_2 b} = D^{(n_1)}_{-a,b} \otimes \mathbb{1}_{n_2}. \tag{24}$$

These are critical observations for what we intend to show. The rightmost identities, which hold factor-by-factor, follow from straightforward calculations. Since

$$\omega^{n_1a}_{2n_1n_2} = \omega^{a}_{2n_2}, \qquad \omega^{n_1b}_{2n_1n_2} = \omega^{b}_{2n_2}, \qquad \omega^{n_2a}_{2n_1n_2} = \omega^{a}_{2n_1}, \qquad \omega^{n_2b}_{2n_1n_2} = \omega^{b}_{2n_1}, \tag{25}$$

we have that

$$D^{(n)}_{da,db} = \begin{pmatrix} \mathbb{1}_{n_1} \otimes D^{(n_2)}_{a,b} & & & \\ & \mathbb{1}_{n_1} \otimes \omega^{a}_{2n_2} D^{(n_2)}_{a,b} & & \\ & & \mathbb{1}_{n_1} \otimes \omega^{b}_{2n_2} D^{(n_2)}_{a,b} & \\ & & & \mathbb{1}_{n_1} \otimes \omega^{a+b}_{2n_2} D^{(n_2)}_{a,b} \end{pmatrix} \tag{26}$$

and

$$D^{(n)}_{(d-2)a,(d-2)b} = \begin{pmatrix} D^{(n_1)}_{-a,b} \otimes \mathbb{1}_{n_2} & & & \\ & \omega^{a}_{2n_1} D^{(n_1)}_{-a,b} \otimes \mathbb{1}_{n_2} & & \\ & & \omega^{b}_{2n_1} D^{(n_1)}_{-a,b} \otimes \mathbb{1}_{n_2} & \\ & & & \omega^{a+b}_{2n_1} D^{(n_1)}_{-a,b} \otimes \mathbb{1}_{n_2} \end{pmatrix}. \tag{27}$$

3.1.1. Block diagonal structure of Π_1 and Π_2. We can now use the decompositions (26) and (27) to show that Π_1 and Π_2 are also block-diagonal, and that the blocks have a particular structure.

The expansions of Π_1 and Π_2 in the displacement operator basis read

$$\Pi_1 = \frac{d(d-1)}{2n} \sum_{a,b=0}^{d-3} \langle\psi_{0,0}|D^{(n)}_{da,db}|\psi_{0,0}\rangle D^{(n)}_{-da,-db}, \tag{28}$$

$$\Pi_2 = \frac{(d-1)}{2d} \sum_{a,b=0}^{d-1} \langle\psi_{0,0}|D^{(n)}_{(d-2)a,(d-2)b}|\psi_{0,0}\rangle D^{(n)}_{-(d-2)a,-(d-2)b}. \tag{29}$$

See appendix C. The displacement operators that occur in these expansions are block-diagonal and, consequently, so are Π_1 and Π_2. We can therefore rewrite equations (19) and (20) as

$$\Pi_1 = \frac{d-1}{2d} \sum_{j=1}^{4} \sum_{a,b=0}^{d-1} D^{(n)}_{(d-2)a,(d-2)b} \Lambda_j |\psi_{0,0}\rangle\langle\psi_{0,0}| \Lambda_j D^{(n)}_{(2-d)a,(2-d)b}, \tag{30}$$

$$\Pi_2 = \frac{d-1}{2(d-2)} \sum_{j=1}^{4} \sum_{a,b=0}^{d-3} D^{(n)}_{da,db} \Lambda_j |\psi_{0,0}\rangle\langle\psi_{0,0}| \Lambda_j D^{(n)}_{-da,-db}, \tag{31}$$

where Λ_j is the orthogonal projection onto the jth subspace. The operator $\Lambda_j|\psi_{0,0}\rangle\langle\psi_{0,0}|\Lambda_j$ can be regarded as an operator on the jth subspace, and, by (26) and (27), the jth block of Π_1 and Π_2 can be written as

$$\Pi_1^j = \frac{d-1}{2d} \sum_{a,b=0}^{d-1} (D^{(n_1)}_{-a,b} \otimes \mathbb{1}_{n_2}) \Lambda_j |\psi_{0,0}\rangle\langle\psi_{0,0}| \Lambda_j (D^{(n_1)}_{a,-b} \otimes \mathbb{1}_{n_2}), \tag{32}$$

$$\Pi_2^j = \frac{d-1}{2(d-2)} \sum_{a,b=0}^{d-3} (\mathbb{1}_{n_1} \otimes D^{(n_2)}_{a,b}) \Lambda_j |\psi_{0,0}\rangle\langle\psi_{0,0}| \Lambda_j (\mathbb{1}_{n_1} \otimes D^{(n_2)}_{-a,-b}). \tag{33}$$

The translation properties (8) allow us to lower the upper limits of the sums:

$$\Pi_1^j = \frac{(d-1)}{n_1} \sum_{a,b=0}^{n_1-1} (D^{(n_1)}_{-a,b} \otimes \mathbb{1}_{n_2}) \Lambda_j |\psi_{0,0}\rangle\langle\psi_{0,0}| \Lambda_j (D^{(n_1)}_{a,-b} \otimes \mathbb{1}_{n_2}), \tag{34}$$

$$\Pi_2^j = \frac{(d-1)}{n_2} \sum_{a,b=0}^{n_2-1} (\mathbb{1}_{n_1} \otimes D^{(n_2)}_{a,b}) \Lambda_j |\psi_{0,0}\rangle\langle\psi_{0,0}| \Lambda_j (\mathbb{1}_{n_1} \otimes D^{(n_2)}_{-a,-b}). \tag{35}$$

Finally, in appendix E, see equations (E.1) and (E.2), we prove that these sums reduce to

$$\Pi_1^j = (d-1)\mathbb{1}_{n_1} \otimes \mathrm{tr}_{n_1}(\Lambda_j|\psi_{0,0}\rangle\langle\psi_{0,0}|\Lambda_j), \tag{36}$$

$$\Pi_2^j = (d-1)\mathrm{tr}_{n_2}(\Lambda_j|\psi_{0,0}\rangle\langle\psi_{0,0}|\Lambda_j) \otimes \mathbb{1}_{n_2}. \tag{37}$$

The traces in (36) and (37) are the partial traces with respect to the splitting of the jth subspace as a tensor product. We use the language of multipartite systems and refer to $(d-1)\mathrm{tr}_{n_1}(\Lambda_j|\psi_{0,0}\rangle\langle\psi_{0,0}|\Lambda_j)$ as the right marginal operator of Π_1^j and to $(d-1)\mathrm{tr}_{n_2}(\Lambda_j|\psi_{0,0}\rangle\langle\psi_{0,0}|\Lambda_j)$ as the left marginal operator of Π_2^j. In the next section we will

prove that if the SIC is aligned, the right marginal operator of Π_1^j is a projection operator, and we will calculate its rank. Then, since the two partial traces have the same spectrum (up to 0s), the left marginal operator of Π_2^j is also a projection operator, and it has the same rank.

3.2. Displaced parity operators

Displaced parity operators will play an important role in our further analysis of the blocks of Π_1 and Π_2. In this section we introduce these operators and describe some of their properties.

A parity operator is a Clifford unitary P for which

$$PD_{a,b}^{(n)}P = D_{-a,-b}^{(n)} \tag{38}$$

holds for all pairs of integers a and b. Here, we have borrowed the terminology from crystallography; for an odd n, if you label the points in an n-periodic 2-dimensional lattice by the indices of the displacement operators, the action of P corresponds to a reflection in the origin. For an even n, the analogy breaks down due to the non-periodicity of the displacement operators, see equation (8). In appendix D we show that, irrespective of n being odd or even, there is (up to a sign) only one Clifford unitary which satisfies (38), namely

$$P^{(n)} = \sum_{u=0}^{n-1} |-u\rangle\langle u|. \tag{39}$$

This may not be so surprising, considering the analogy with crystallography, but the proof is a good illustration of the difference in complexity between even and odd dimensions. The essential uniqueness justifies calling $P^{(n)}$ *the parity operator*. In the definition (39), $\{|u\rangle : u \in \mathbb{Z}_n\}$ is an orthonormal basis relative to which X_n and Z_n are represented as in equation (4).

The definition (38) seems to depend on the representation of the Weyl–Heisenberg group. However, as was pointed out in section 2.1.3, the Clifford groups associated with different representations are canonically unitary equivalent, and the canonical isomorphism between the Clifford groups connects the two parity operators. Therefore, the parity operator can be defined by (39) in any representation, although the basis on the righ-hand side is representation-dependent.

The parity operator is an involution. Recall that an involution is an operator which squares to the identity operator. Involutions are diagonalizable and each eigenvalue equals either $+1$ or -1. The multiplicities are determined by the trace of the involution; if I is an involution on an n-dimensional Hilbert space, the multiplicity of the eigenvalue $+1$ is $(n + \mathrm{tr}I)/2$ and the multiplicity of -1 is $(n - \mathrm{tr}I)/2$. We write, for short,

$$\mathrm{spec}\, I = \left(\frac{n + \mathrm{tr}I}{2}, \frac{n - \mathrm{tr}I}{2}\right). \tag{40}$$

The trace of the parity operator is 1 if n is odd and 2 if n is even. Consequently,

$$\mathrm{spec}\, P^{(n)} = \begin{cases} \left(\frac{n+1}{2}, \frac{n-1}{2}\right) & \text{if } n \text{ is odd,} \\ \left(\frac{n+2}{2}, \frac{n-2}{2}\right) & \text{if } n \text{ is even.} \end{cases} \tag{41}$$

By displacing $P^{(n)}$ we can generate new involutions in the Clifford group:

$$P_{a,b}^{(n)} = D_{a,b}^{(n)}P^{(n)}. \tag{42}$$

If n is odd, the displaced parity operators are unitarily equivalent to, and hence isospectral to, $P^{(n)}$. For in the odd case, $2k = a$ and $2l = b$ can always be solved in arithmetic modulo n, and by equations (6) and (38), $P^{(n)}_{a,b} = D^{(n)}_{k,l} P^{(n)} D^{(n)}_{-k,-l}$. In the analogy with crystallography, $P^{(n)}_{a,b}$ corresponds to a reflection in the point (k, l). If n is even, however, the situation is more complicated. In the even case, it is not only the identity operator that is preserved by the action of P, and the displaced parity operators divide into two unitary conjugacy classes. Irrespective of the parity of n we have that

$$\mathrm{tr}P^{(n)}_{a,b} = \sum_{u=0}^{n-1} \tau_n^{ab} \langle -u|X^a Z^b|u\rangle = \sum_{u=0}^{n-1} \tau_n^{ab+2bu} \delta^{(n)}_{2u+a,0}, \tag{43}$$

where $\delta^{(n)}_{\cdot,\cdot}$ is the Kronecker delta in arithmetic modulo n. Evaluation of the right-hand side for all possible values of n, a, and b yields

$$\mathrm{tr}P^{(n)}_{a,b} = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ 1 - (-1)^{(a+1)(b+1)} & \text{if } n \text{ is even.} \end{cases} \tag{44}$$

We see that, in the even case, the trace of a displaced parity operator can be 0 or 2. If $\mathrm{tr}P^{(n)}_{a,b} = 2$, then a and b have to be even, say $a = 2k$ and $b = 2l$, and $P^{(n)}_{a,b} = D^{(n)}_{k,l} P^{(n)} D^{(n)}_{-k,-l}$. However, if $\mathrm{tr}P^{(n)}_{a,b} = 0$, then $P^{(n)}_{a,b}$ is not unitarily equivalent to $P^{(n)}$.

An immediate consequence of equations (40) and (44) is that

$$\mathrm{spec}P^{(n)}_{a,b} = \begin{cases} \left(\frac{n+1}{2}, \frac{n-1}{2}\right) & \text{if } n \text{ is odd,} \\ \left(\frac{n+1-(-1)^{(a+1)(b+1)}}{2}, \frac{n-1+(-1)^{(a+1)(b+1)}}{2}\right) & \text{if } n \text{ is even.} \end{cases} \tag{45}$$

Since the expansion of the parity operator in the displacement operator basis is

$$P^{(n)} = \frac{1}{n} \sum_{a,b=0}^{n-1} \mathrm{tr}\left(P^{(n)}_{a,b}\right) D^{(n)}_{-a,-b}, \tag{46}$$

we also conclude from (44) that

$$P^{(n)} = \begin{cases} \frac{1}{n} \sum_{a,b=0}^{n-1} D^{(n)}_{a,b} & \text{if } n \text{ is odd,} \\ \frac{1}{n} \sum_{a,b=0}^{n-1} (1 - (-1)^{(a+1)(b+1)}) D^{(n)}_{a,b} & \text{if } n \text{ is even.} \end{cases} \tag{47}$$

Equation (47) is the key observation used in the next section.

3.3. *Proof that* Π_1 *is a projection operator*

So far, we have not used the assumption that the SIC is aligned. In this section we will do so and calculate the blocks of Π_1. More precisely, we will show that

$$\Pi_1^1 = \frac{1}{2} \mathbb{1}_{n_1} \otimes (\mathbb{1}_{n_2} \mp P^{(n_2)}_{0,0}), \tag{48}$$

$$\Pi_1^2 = \frac{1}{2} \mathbb{1}_{n_1} \otimes (\mathbb{1}_{n_2} \pm P^{(n_2)}_{0,1}), \tag{49}$$

$$\Pi_1^3 = \frac{1}{2} \mathbb{1}_{n_1} \otimes (\mathbb{1}_{n_2} \pm P^{(n_2)}_{-1,0}), \tag{50}$$

$$\Pi_1^4 = \frac{1}{2}\mathbb{1}_{n_1} \otimes (\mathbb{1}_{n_2} \pm P_{-1,1}^{(n_2)}). \tag{51}$$

The upper signs are to be used if n_2 is odd and the lower signs are to be used if n_2 is even. Before that, however, let us consider some consequences of these identities.

3.3.1. Consequences of equations (48)–(51). Let us prove that the frames (17) and (18) are tight, given that the blocks of Π_1 satisfy (48)–(51). Since the displaced parity operators are involutions, the blocks of Π_1, and hence Π_1 itself, are projection operators. We calculate their ranks.

If n_2 is odd, then, by (45), Π_1^1 has rank $n_1(n_2-1)/2$ while Π_1^2, Π_1^3, and Π_1^4 each have rank $n_1(n_2+1)/2$. If n_2 is even, Π_1^1 has rank $n_1(n_2+2)/2$ while Π_1^2, Π_1^3, and Π_1^4 each have rank $n_1n_2/2$. In either case,

$$\mathrm{rank}\Pi_1 = \frac{n_1(n_2-1)}{2} + \frac{3n_1(n_2+1)}{2} = \frac{n_1(n_2+2)}{2} + \frac{3n_1n_2}{2} = \frac{d(d-1)}{2}. \tag{52}$$

Next we consider the operator Π_2. Since the blocks of Π_1 are projection operators, so are the blocks of Π_2, as well as Π_2 itself; for equations (36) and (37) say that the left marginal operator of Π_2^j has the same spectrum as the right marginal operator of Π_1^j. We conclude that if n_2 is odd, Π_2^1 has rank $n_2(n_2-1)/2$ while Π_2^2, Π_2^3, and Π_2^4 each have rank $n_2(n_2+1)/2$, and if n_2 is even, Π_2^1 has rank $n_2(n_2+2)/2$ while Π_2^2, Π_2^3, and Π_2^4 each have rank $n_2^2/2$. In either case,

$$\mathrm{rank}\Pi_2 = \frac{n_2(n_2-1)}{2} + \frac{3n_2(n_2+1)}{2} = \frac{n_2(n_2+2)}{2} + \frac{3n_2^2}{2} = \frac{(d-1)(d-2)}{2}. \tag{53}$$

We have shown that, under the assumption that equations (48)–(51) hold, an aligned SIC in dimension $d(d-2)$ contains a tight d^2-frame of rank $d(d-1)/2$ and a tight $(d-2)^2$-frame of rank $(d-1)(d-2)/2$. By displacing these frames we will generate the whole SIC. In other words, the SIC consists of $(d-2)^2$ tight d^2-frames, and, alternatively, of d^2 tight $(d-2)^2$-frames. In the following section we expand on the proof of the structure of Π_1. Afterwards we discuss implications on the symmetry of aligned SICs.

3.3.2. Derivations of equations (48)–(51). Using definition (14), the expansion (28) can be rearranged as

$$\Pi_1 = \frac{1}{2}\mathbb{1}_{n_2} + \frac{1}{4n_2}\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta_{da,db}^{(n)}} D_{-da,-db}^{(n)}. \tag{54}$$

Then, by (26), the blocks of Π_1 are given by

$$\Pi_1^1 = \frac{1}{2}\mathbb{1}_{n_1} \otimes \left(\mathbb{1}_{n_2} + \frac{1}{2n_2}\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta_{da,db}^{(n)}} D_{a,b}^{(n_2)}\right), \tag{55}$$

$$\Pi_1^2 = \frac{1}{2}\mathbb{1}_{n_1} \otimes \left(\mathbb{1}_{n_2} + \frac{1}{2n_2}\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta_{da,db}^{(n)}} \omega_{2n_2}^{a} D_{a,b}^{(n_2)}\right), \tag{56}$$

$$\Pi_1^3 = \frac{1}{2}\mathbb{1}_{n_1} \otimes \left(\mathbb{1}_{n_2} + \frac{1}{2n_2}\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta_{da,db}^{(n)}} \omega_{2n_2}^{b} D_{a,b}^{(n_2)}\right), \tag{57}$$

$$\Pi_1^4 = \frac{1}{2}\mathbb{1}_{n_1} \otimes \left(\mathbb{1}_{n_2} + \frac{1}{2n_2}\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} \omega_{2n_2}^{a+b} D^{(n_2)}_{a,b}\right). \tag{58}$$

We will now prove that, under the alignment assumption (15), these expressions equal those in equations (48)–(51).

According to the alignment assumption, the overlap phases for the displacement operators appearing in the expansion (54) of Π_1 are

$$\mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} = -(-1)^{(a+1)(b+1)}. \tag{59}$$

(Notice that this formula holds if $a = 0 \mod (d-2)$ and $b = 0 \mod (d-2)$ as well). The overlap phases satisfy the translation properties

$$\mathrm{e}^{\mathrm{i}\theta^{(n)}_{d(a+m),db}} = \begin{cases} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} & \text{if } m \text{ is even,} \\ \mathrm{e}^{\mathrm{i}\theta^{(n)}_{d(a+1),db}} & \text{if } m \text{ is odd,} \end{cases} \tag{60}$$

and

$$\mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,d(b+m)}} = \begin{cases} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} & \text{if } m \text{ is even,} \\ \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,d(b+1)}} & \text{if } m \text{ is odd.} \end{cases} \tag{61}$$

Using these, the translation properties (8), and the identity $\omega_{2n_2}^{m+n_2} = -\omega_{2n_2}^{m}$, one can reduce the upper limits in the sums in equations (55)–(58) to $n_2 - 1$. More precisely, one can show that if n_2 is odd, then

$$\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} D^{(n_2)}_{a,b} = -2\sum_{a,b=0}^{n_2-1} D^{(n_2)}_{a,b}, \tag{62}$$

$$\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} \omega_{2n_2}^{a} D^{(n_2)}_{a,b} = 2\sum_{a,b=0}^{n_2-1} \tau_{n_2}^{a} D^{(n_2)}_{a,b}, \tag{63}$$

$$\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} \omega_{2n_2}^{b} D^{(n_2)}_{a,b} = 2\sum_{a,b=0}^{n_2-1} \tau_{n_2}^{b} D^{(n_2)}_{a,b}, \tag{64}$$

$$\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} \omega_{2n_2}^{a+b} D^{(n_2)}_{a,b} = 2\sum_{a,b=0}^{n_2-1} \tau_{2n_2}^{a+b} D^{(n_2)}_{a,b}, \tag{65}$$

and if n_2 is even,

$$\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} D^{(n_2)}_{a,b} = \sum_{a,b=0}^{n_2-1} (1-(-1)^{(a+1)(b+1)}) D^{(n_2)}_{a,b}, \tag{66}$$

$$\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} \omega_{2n_2}^{a} D^{(n_2)}_{a,b} = \sum_{a,b=0}^{n_2-1} ((-1)^a+1)((-1)^b-1) \tau_{n_2}^{a} D^{(n_2)}_{a,b}, \tag{67}$$

$$\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} \omega_{2n_2}^{b} D^{(n_2)}_{a,b} = \sum_{a,b=0}^{n_2-1} ((-1)^a - 1)((-1)^b + 1)\tau_{n_2}^{b} D^{(n_2)}_{a,b}, \tag{68}$$

$$\sum_{a,b=0}^{d-3} \mathrm{e}^{\mathrm{i}\theta^{(n)}_{da,db}} \omega_{2n_2}^{a+b} D^{(n_2)}_{a,b} = -\sum_{a,b=0}^{n_2-1} ((-1)^a - 1)((-1)^b - 1)\tau_{n_2}^{a+b} D^{(n_2)}_{a,b}. \tag{69}$$

Equation (48) follows immediately from (55) and a comparison between equations (47) and (62) in the odd case, and between equations (47) and (66) in the even case.

Next, we consider the equations (63) and (67). If n_2 is odd, then

$$\sum_{a,b=0}^{n_2-1} \tau_{n_2}^{a} D^{(n_2)}_{a,b} = \sum_{a,b=0}^{n_2-1} D^{(n_2)}_{a,b+1} Z_{n_2}^{-1} = \sum_{a,b=0}^{n_2-1} D^{(n_2)}_{a,b} Z_{n_2}^{-1} = n_2 P^{(n_2)} Z_{n_2}^{-1} = n_2 P^{(n_2)}_{0,1}. \tag{70}$$

The second identity follows from the translation property (8), the third from equation (47), and the fourth from (38). If n_2 is even, then

$$\begin{aligned}\sum_{a,b=0}^{n_2-1} ((-1)^a + 1)((-1)^b - 1)\tau_{n_2}^{a} D^{(n_2)}_{a,b} &= \sum_{a,b=0}^{n_2-1} ((-1)^a + 1)((-1)^b - 1) D^{(n_2)}_{a,b+1} Z_{n_2}^{-1} \\ &= -2\sum_{a,b=0}^{n_2-1} (1 - (-1)^{(a+1)(b+1)}) D^{(n_2)}_{a,b} Z_{n_2}^{-1}.\end{aligned} \tag{71}$$

Again, in the second identity we used (8), and we rewrote the factors in front of the displacement operators. Using equations (47) and (38), we identify the right-hand side of (71) as $-2n_2 P^{(n_2)}_{0,1}$. This finishes the proof of equation (49). The proofs of equations (50) and (51) are similar to the proof of (49) and, hence, we omit them.

4. Symmetry

By a symmetry of a SIC we mean any unitary which permutes the SIC vectors. In this section we show that any aligned WH-SIC in dimension $n = d(d-2)$, where d is even, has a symplectic symmetry of order 2 which leaves unchanged a SIC fiducial satisfying the alignment condition (15). The corresponding result for d odd was proven in [7].

In section 3.1 we have shown that the Hilbert space can be decomposed into four subspaces, each admitting a tensor product splitting relative to which the blocks of Π_1 acquire the form in equation (36). It follows from equation (36) and equations (48)–(51) that

$$\mathrm{tr}_{n_1}(\Lambda_j|\psi_{0,0}\rangle\langle\psi_{0,0}|\Lambda_j) = \frac{1}{2(d-1)}(\mathbb{1}_{n_2} + P_j) \tag{72}$$

where

$$P_1 = \mp P^{(n_2)}_{0,0}, \qquad P_2 = \pm P^{(n_2)}_{0,1}, \qquad P_3 = \pm P^{(n_2)}_{-1,0}, \qquad P_4 = \pm P^{(n_2)}_{-1,1}. \tag{73}$$

Recall that the upper signs are to be used if n_2 is odd and the lower signs are to be used if n_2 is even. We fix an orthonormal basis $\{|f_u; j\rangle : u \in \mathbb{Z}_{n_2}\}$ in the second factor of the jth subspace which diagonalizes P_j in such a way that its eigenvalues are arranged in descending order:

$$P_j = \sum_{u=0}^{m_j-1} |f_u;j\rangle\langle f_u;j| - \sum_{u=0}^{n_2-m_j} |f_u;j\rangle\langle f_u;j|. \tag{74}$$

The upper limits are determined by equation (45). That is,

$$m_1 = \begin{cases} (n_2-1)/2 & \text{if } n_2 \text{ is odd,} \\ (n_2-1)/2 & \text{if } n_2 \text{ is even,} \end{cases} \tag{75}$$

and

$$m_2 = m_3 = m_4 = \begin{cases} (n_2+1)/2 & \text{if } n_2 \text{ is odd,} \\ n_2/2 & \text{if } n_2 \text{ is even.} \end{cases} \tag{76}$$

The diagonalizing bases for the parity operators can be completed to Schmidt-bases for the projections of the SIC fiducial [21]. According to equation (72) there thus exist mutually orthogonal unit vectors $|e_u;j\rangle$ in the first factor in the jth subspace such that

$$\Lambda_j|\psi_{0,0}\rangle = \frac{1}{\sqrt{d-1}} \sum_{u=0}^{m_j} |e_u;j\rangle \otimes |f_u;j\rangle. \tag{77}$$

Define a unitary U_b by

$$U_b = \begin{pmatrix} \mathbb{1}_{n_1} \otimes P_{0,0}^{(n_2)} & & & \\ & -\mathbb{1}_{n_1} \otimes P_{0,1}^{(n_2)} & & \\ & & -\mathbb{1}_{n_1} \otimes P_{-1,0}^{(n_2)} & \\ & & & -\mathbb{1}_{n_1} \otimes P_{-1,1}^{(n_2)} \end{pmatrix}. \tag{78}$$

The unitary clearly leaves the SIC fiducial unchanged and is of second order, since the parity operators are of second order. If, in addition, U_b permutes the other SIC vectors, it is a symmetry. This is the case if U_b belongs to the Clifford group. We next prove that U_b is, in fact, the symplectic unitary corresponding to

$$F_b = \begin{pmatrix} 1-d & n \\ n & 1-d+n \end{pmatrix} = \begin{pmatrix} -n & 1-d \\ d-1-n & n \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tag{79}$$

the product in the right-hand side being a prime decomposition of F_b in $\mathrm{SL}(2,\mathbb{Z}_{\bar{n}})$. The choice of symplectic matrix is inspired by a conjecture of Scott and Grassl [4, 22].

The inverse of $1-d$ modulo $\bar{n}$ is $(1-d)(n+1)$. Applying (12) and (11) yields

$$V_{F_b} = \sum_{u=0}^{n-1} (-1)^u |u\rangle\langle dn_2 - (d-1)u|. \tag{80}$$

The expansion of V_{F_b} in the displacement operator basis then reads

$$\begin{aligned} V_{F_b} &= \frac{1}{n} \sum_{a,b=0}^{n-1} \sum_{u=0}^{n-1} (-1)^u \langle dn_2 - (d-1)u|D_{a,b}^{(n)}|u\rangle D_{-a,-b}^{(n)} \\ &= \frac{1}{n} \sum_{a,b=0}^{n-1} \sum_{u=0}^{n-1} (-1)^u \tau_n^{ab} \omega_n^{bu} \langle dn_2 - (d-1)u|u+a\rangle D_{-a,-b}^{(n)} \\ &= \frac{1}{n} \sum_{a,b=0}^{n-1} \sum_{u=0}^{n-1} (-1)^u \tau_n^{ab} \omega_n^{bu} \delta_{a,dn_2-du}^{(n)} D_{-a,-b}^{(n)}. \end{aligned} \tag{81}$$

The Kronecker delta is non-zero only if a is divisible by d and $u = n_2 - a/d \bmod 2n_2$. Hence, we can rewrite the expansion of V_{F_b} as

$$\begin{aligned}
V_{F_b} &= \frac{1}{n}\sum_{a=0}^{d-3}\sum_{b=0}^{n-1}\sum_{k=0}^{d-1}(-1)^{u}\tau_n^{dab}\omega_n^{bu}\delta^{(n)}_{a,n_2-u}D^{(n)}_{-da,-b} \\
&= \frac{1}{n}\sum_{a=0}^{n_2}\sum_{b=0}^{n-1}\sum_{k=0}^{d-1}(-1)^{n_2-a}\tau_n^{dab}\omega_n^{b(n_2-a)}\omega_n^{2bn_2k}D^{(n)}_{-da,-b} \\
&\quad + \frac{1}{n}\sum_{a=n_1}^{d-3}\sum_{b=0}^{n-1}\sum_{k=1}^{d}(-1)^{n_2-a}\tau_n^{dab}\omega_n^{b(n_2-a)}\omega_n^{2bn_2k}D^{(n)}_{-da,-b} \\
&= \frac{1}{d-2}\sum_{a=0}^{n_2}\sum_{b=0}^{n-1}(-1)^{n_2-a}\tau_n^{dab}\omega_n^{b(n_2-a)}\delta^{(d)}_{b,0}D^{(n)}_{-da,-b} \\
&\quad + \frac{1}{d-2}\sum_{a=n_1}^{d-3}\sum_{b=0}^{n-1}(-1)^{n_2-a}\tau_n^{dab}\omega_n^{b(n_2-a)}\omega_d^{b}\delta^{(d)}_{b,0}D^{(n)}_{-da,-b} \\
&= \frac{1}{d-2}\sum_{a=0}^{d-3}\sum_{b=0}^{n-1}(-1)^{n_2-a}\tau_n^{dab}\omega_n^{b(n_2-a)}\delta^{(d)}_{b,0}D^{(n)}_{-da,-b}. \qquad (82)
\end{aligned}$$

Only those terms in which b is divisible by d are thus non-zero and, hence,

$$\begin{aligned}
V_{F_b} &= \frac{1}{d-2}\sum_{a,b=0}^{d-3}(-1)^{n_2-a}\tau_n^{d^2ab}\omega_n^{db(n_2-a)}D^{(n)}_{-da,-db} \\
&= \frac{1}{d-2}\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}D^{(n)}_{-da,-db}. \qquad (83)
\end{aligned}$$

According to equation (26), V_{F_b} is block-diagonal and the blocks split:

$$\begin{aligned}
V_{F_b} =& \frac{1}{d-2}\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab} \\
&\begin{pmatrix}
\mathbb{1}_{n_1}\otimes D^{(n_2)}_{-a,-b} & & & \\
& \mathbb{1}_{n_1}\otimes\omega_{2n_2}^{-a}D^{(n_2)}_{-a,-b} & & \\
& & \mathbb{1}_{n_1}\otimes\omega_{2n_2}^{-b}D^{(n_2)}_{-a,-b} & \\
& & & \mathbb{1}_{n_1}\otimes\omega_{2n_2}^{-(a+b)}D^{(n_2)}_{-a,-b}
\end{pmatrix}. \qquad (84)
\end{aligned}$$

Direct calculations using the translation properties (8) yield that if n_2 is odd,

$$\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}D^{(n_2)}_{-a,-b} = 2\sum_{a,b=0}^{n_2-1}D^{(n_2)}_{-a,-b}, \qquad (85)$$

$$\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\omega_{2n_2}^{-a}D^{(n_2)}_{-a,-b} = -2\sum_{a,b=0}^{n_2-1}\tau_{n_2}^{-a}D^{(n_2)}_{-a,-b}, \qquad (86)$$

$$\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\omega_{2n_2}^{-b}D^{(n_2)}_{-a,-b}=-2\sum_{a,b=0}^{n_2-1}\tau_{n_2}^{-b}D^{(n_2)}_{-a,-b}, \tag{87}$$

$$\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\omega_{2n_2}^{-(a+b)}D^{(n_2)}_{-a,-b}=-2\sum_{a,b=0}^{n_2-1}\tau_{n_2}^{-(a+b)}D^{(n_2)}_{-a,-b}, \tag{88}$$

and if n_2 is even,

$$\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}D^{(n_2)}_{-a,-b}=2\sum_{a,b=0}^{n_2-1}(1-(-1)^{(a+1)(b+1)})D^{(n_2)}_{-a,-b}, \tag{89}$$

$$\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\omega_{2n_2}^{-a}D^{(n_2)}_{-a,-b}=-\sum_{a,b=0}^{n_2-1}(1+(-1)^{a})(1-(-1)^{b})\omega_{2n_2}^{-a}D^{(n_2)}_{-a,-b}, \tag{90}$$

$$\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\omega_{2n_2}^{-b}D^{(n_2)}_{-a,-b}=-\sum_{a,b=0}^{n_2-1}(1-(-1)^{a})(1+(-1)^{b})\omega_{2n_2}^{-b}D^{(n_2)}_{-a,-b}, \tag{91}$$

$$\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\omega_{2n_2}^{-(a+b)}D^{(n_2)}_{-a,-b}=-\sum_{a,b=0}^{n_2-1}(1-(-1)^{a})(1-(-1)^{b})\omega_{2n_2}^{-(a+b)}D^{(n_2)}_{-a,-b}. \tag{92}$$

The right-hand sides in (85) and (89) equal $2n_2P^{(n_2)}_{0,0}$, see equation (47), and, hence, the first block of V_{F_b} is

$$\frac{1}{d-2}\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\mathbb{1}_{n_1}\otimes D^{(n_2)}_{-a,-b}=\mathbb{1}_{n_1}\otimes P^{(n_2)}_{0,0}. \tag{93}$$

Furthermore, by a comparison with equations (70) and (71), we see that, irrespective of the parity of n_2, the second block of V_{F_b} is

$$\frac{1}{d-2}\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\mathbb{1}_{n_1}\otimes \omega_{2n_2}^{-a}D^{(n_2)}_{-a,-b}=-\mathbb{1}_{n_1}\otimes P^{(n_2)}_{0,1}. \tag{94}$$

Similarly, one can show that the third and fourth blocks of V_{F_b} are

$$\frac{1}{d-2}\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\mathbb{1}_{n_1}\otimes \omega_{2n_2}^{-a}D^{(n_2)}_{-a,-b}=-\mathbb{1}_{n_1}\otimes P^{(n_2)}_{-1,0}, \tag{95}$$

$$\frac{1}{d-2}\sum_{a,b=0}^{d-3}(-1)^{n_2+a+b+ab}\mathbb{1}_{n_1}\otimes \omega_{2n_2}^{-(a+b)}D^{(n_2)}_{-a,-b}=-\mathbb{1}_{n_1}\otimes P^{(n_2)}_{-1,1}, \tag{96}$$

respectively. This proves that $U_b=V_{F_b}$.

5. Conclusion

We have proven that the property of alignment of WH-SICs in even dimensions of the form $d(d-2)$ implies that the SICs can be partitioned into sets of equiangular tight frames, in two different ways. Together with [7], which proves the same for SICs in odd dimensions of the form $d(d-2)$, this concludes the proof of the implication for all aligned WH-SICs.

The proof in [7] employs a powerful tool for handling the Weyl–Heisenberg group in composite dimensions, namely Chinese remaindering. In the past, Chinese remaindering has only been successfully used for Hilbert spaces of composite dimensions where the factors are relatively prime. In this paper, we have used special properties of irreducible representations of the Weyl–Heisenberg group in dimensions divisible by 4 to decompose the Hilbert space into four subspaces, and to apply Chinese remaindering in each of them. Thus we have extended the use of Chinese remaindering to composite dimensions where the factors are not relatively prime. A generalization of our procedure to all composite dimensions is not immediately available. However, decomposing the Hilbert space into a direct sum presents itself as a natural tool for tackling composite dimensions with Chinese remaindering, and it will be interesting to see whether it can be employed in other cases.

Finally, we have proved that an extra symmetry, conjectured for aligned SICs and proven in [7] for the odd-dimensional case, is indeed always present in the aligned SICs.

Acknowledgments

The authors thank Ingemar Bengtsson for proposing the problem addressed in the current paper, for providing the representation in appendix A, for suggesting improvements to the text, and for numerous fruitful discussions. We also thank Marcus Appleby for sharing his notes on Chinese remaindering with us.

Appendix A. An unorthodox representation of the Weyl–Heisenberg group

In this appendix, we prove that if the dimension of the Hilbert space is divisible by 4, the space can be decomposed into 4 subspaces in such a way that the displacement operators with even indices assume the block-diagonal form in equation (21).

Let $\mathcal{H}^n$ be an n-dimensional Hilbert space. Assume that n is divisible by 4 and write $n = 4m$. Fix an orthonormal basis $\{|u;j\rangle : u \in \mathbb{Z}_m, j = 1,\dots,4\}$ for $\mathcal{H}^n$, which we assume to be lexicographically ordered, and write $\mathcal{H}^m_j$ for the linear span of $\{|u;j\rangle : u \in \mathbb{Z}_m\}$. Furthermore, define operators $\mathbb{1}^{ji}_m$, X^{ji}_m, and Z^{ji}_m from $\mathcal{H}^m_i$ onto $\mathcal{H}^m_j$ by

$$\mathbb{1}^{ji}_m = \sum_{u=0}^{m-1} |u;j\rangle\langle u;i|, \qquad X^{ji}_m = \sum_{u=0}^{m-1} |u+1;j\rangle\langle u;i|, \qquad Z^{ji}_m = \sum_{u=0}^{m-1} \omega_m^u |u;j\rangle\langle u;i|, \tag{A.1}$$

and let Λ_j be the orthogonal projection of $\mathcal{H}^n$ onto $\mathcal{H}^n_j$.

The operators X^{jj}_m and Z^{jj}_m define irreducible representations of $\mathrm{WH}(m)$ on $\mathcal{H}^m_j$. Inspired by [23], we define an m-nomial unitary representation of $\mathrm{WH}(n)$ on $\mathcal{H}^n$ by declaring that

$$X_n = \begin{pmatrix} 0 & 0 & X^{13}_m & 0 \\ 0 & 0 & 0 & \omega_{2m} X^{24}_m \\ \mathbb{1}^{31}_m & 0 & 0 & 0 \\ 0 & \mathbb{1}^{42}_m & 0 & 0 \end{pmatrix}, \qquad Z_n = \begin{pmatrix} 0 & \mathbb{1}^{12}_m & 0 & 0 \\ Z^{21}_m & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega_{4m}\mathbb{1}^{34}_m \\ 0 & 0 & \omega_{4m} Z^{43}_m & 0 \end{pmatrix}. \tag{A.2}$$

In these matrix representations, the operators on position (j,i) correspond to $\Lambda_j X_n \Lambda_i$ and $\Lambda_j Z_n \Lambda_i$, respectively, regarded as operators from $\mathcal{H}_i^m$ to $\mathcal{H}_j^m$. Below we will show that the representation defined by equation (A.2) is irreducible. But before we do that, let us emphasize an important feature of the representation and discuss one crucial implication which is key in this paper.

A straightforward calculation shows that the displacement operators on $\mathcal{H}^n$ (i.e. those associated with the representation in (A.2)) with even indices are block-diagonal with respect to the decomposition of $\mathcal{H}^n$ into the four mutually orthogonal subspaces $\mathcal{H}_j^m$:

$$D_{2a,2b}^{(n)} = (-1)^{ab} \begin{pmatrix} D_{a,b}^{(m;1)} & & & \\ & \omega_m^a D_{a,b}^{(m;2)} & & \\ & & \omega_m^b D_{a,b}^{(m;3)} & \\ & & & \omega_m^{a+b} D_{a,b}^{(m;4)} \end{pmatrix}. \tag{A.3}$$

The displacement operator $D_{a,b}^{(m;j)}$ in the right-hand side is the displacement operation associated with the representation of $\mathrm{WH}(m)$ on $\mathcal{H}_j^m$ specified by X_m^{jj} and Z_m^{jj}. Then, by unitary equivalence, see section 2.3, for *any* irreducible representation of $\mathrm{WH}(n)$ on $\mathcal{H}^n$ there exists a decomposition of $\mathcal{H}^n$ into four mutually orthogonal m-dimensional subspaces, and irreducible representations of $\mathrm{WH}(m)$ on these subspaces, such that the displacement operators with even indices of the $\mathrm{WH}(n)$ representation assume a block-diagonal form like in (A.3).

We will now prove that the representation specified by equation (A.2) is irreducible. We do this by proving that it is unitarily equivalent to the 'standard' representation of $\mathrm{WH}(n)$, in which the unitary operators corresponding to X and Z are represented by generalized Pauli matrices, see equation (4). To this end we introduce, for any integer $s \geqslant 2$, two $s \times s$ matrices

$$\mathbb{X}_s = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \qquad \mathbb{Z}_s = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega_s & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \omega_s^{s-1} \end{pmatrix}, \tag{A.4}$$

where, as usual, $\omega_s = \mathrm{e}^{2\pi \mathrm{i}/s}$. We also introduce two unitary $2s \times 2s$ matrices

$$\mathbb{V}_{2s} = \begin{pmatrix} \mathbb{V} & \mathbf{0} \\ \mathbf{0} & \mathbb{V} \end{pmatrix}, \qquad \mathbb{W}_{2s} = \begin{pmatrix} \mathbb{F}_s & 0 \\ 0 & \mathbb{F}_s \end{pmatrix}. \tag{A.5}$$

The bold zeroes denote columns of $(s-1)$ zeros, and $\mathbb{V}$ and $\mathbb{F}_s$ are the $s \times (2s-1)$ matrix and the $s \times s$ matrix, respectively, given by

$$\mathbb{V} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \mathbb{F}_s = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_s & \omega_s^2 & \cdots & \omega_s^{s-1} \\ 1 & \omega_s^2 & \omega_s^4 & \cdots & \omega_s^{2(s-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega_s^{s-1} & \omega_s^{2(s-1)} & \cdots & \omega_s^{(s-1)^2} \end{pmatrix}. \tag{A.6}$$

The matrix $\mathbb{V}_{2s}$ satisfies

$$\mathbb{V}_{2s}\begin{pmatrix}0 & \mathbb{X}_s\\ \mathbb{I}_s & 0\end{pmatrix}\mathbb{V}_{2s}^\dagger = \mathbb{X}_{2s}, \qquad \mathbb{V}_{2s}\begin{pmatrix}\mathbb{Z}_s & 0\\ 0 & \omega_{2s}\mathbb{Z}_s\end{pmatrix}\mathbb{V}_{2s}^\dagger = \mathbb{Z}_{2s}, \tag{A.7}$$

where $\mathbb{I}_s$ is the $s\times s$ identity matrix. Moreover, the matrix $\mathbb{F}_s$, which is the discrete $s\times s$ Fourier transform, satisfies

$$\mathbb{F}_s\mathbb{X}_s\mathbb{F}_s^\dagger = \mathbb{Z}_s, \qquad \mathbb{F}_s\mathbb{Z}_s\mathbb{F}_s^\dagger = \mathbb{X}_s^\dagger. \tag{A.8}$$

To prove the second equality, first note that the square of the Fourier transform is the parity operator, see equation (39), and then use the property (38). The matrix $\mathbb{W}_{2s}$ satisfies

$$\mathbb{W}_{2s}\begin{pmatrix}\mathbb{X}_s & 0\\ 0 & \omega_{2s}\mathbb{X}_s\end{pmatrix}\mathbb{W}_{2s}^\dagger = \begin{pmatrix}\mathbb{Z}_s & 0\\ 0 & \omega_{2s}\mathbb{Z}_s\end{pmatrix}, \qquad \mathbb{W}_{2s}\begin{pmatrix}0 & \mathbb{I}_s\\ \mathbb{Z}_s & 0\end{pmatrix}\mathbb{W}_{2s}^\dagger = \begin{pmatrix}0 & \mathbb{I}_s\\ \mathbb{X}_s^\dagger & 0\end{pmatrix}. \tag{A.9}$$

The unitary $\mathbb{U}_n$, defined as

$$\mathbb{U}_n = \mathbb{V}_{4m}\begin{pmatrix}\mathbb{F}_{2m}^\dagger\mathbb{V}_{2m}\mathbb{W}_{2m} & 0\\ 0 & \mathbb{F}_{2m}^\dagger\mathbb{V}_{2m}\mathbb{W}_{2m}\end{pmatrix}, \tag{A.10}$$

is then such that

$$\mathbb{U}_n\begin{pmatrix}0 & 0 & \mathbb{X}_m & 0\\ 0 & 0 & 0 & \omega_{2m}\mathbb{X}_m\\ \mathbb{I}_m & 0 & 0 & 0\\ 0 & \mathbb{I}_m & 0 & 0\end{pmatrix}\mathbb{U}_n^\dagger = \mathbb{X}_n, \qquad \mathbb{U}_n\begin{pmatrix}0 & \mathbb{I}_m & 0 & 0\\ \mathbb{Z}_m & 0 & 0 & 0\\ 0 & 0 & 0 & \omega_{4m}\mathbb{I}_m\\ 0 & 0 & \omega_{4m}\mathbb{Z}_m & 0\end{pmatrix}\mathbb{U}_n^\dagger = \mathbb{Z}_n. \tag{A.11}$$

We let U_n be the unitary operator on $\mathcal{H}^n$ which is represented by the matrix $\mathbb{U}_n$ relative to the chosen basis for $\mathcal{H}^n$. By equations (A.2) and (A.11), $U_nX_nU_n^\dagger$ and $U_nZ_nU_n^\dagger$ are represented by generalized Pauli matrices.

Appendix B. Chinese remaindering

In this appendix, we present an application of the classic Chinese Remainder Theorem to representations of the Weyl–Heisenberg group. Gross, who came up with the idea, called the application 'Chinese remaindering' [11]. Hence the title of the appendix. The presentation is inspired by [24].

Let n_1 and n_2 be two positive and relatively prime integers and set $m = n_1n_2$. The Chinese remainder theorem states that the rings $\mathbb{Z}_m$ and $\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}$ are isomorphic. An isomorphism is given by

$$u \bmod m \to (u \bmod n_1, u \bmod n_2). \tag{B.1}$$

For simplicity, we will write u for $u \bmod m$ and, then, write u_1 for $u \bmod n_1$ and u_2 for $u \bmod n_2$. We also define $\bar{m}$, $\bar{n}_1$, and $\bar{n}_2$ by

$$\bar{m} = \begin{cases} m & \text{if } m \text{ is odd,}\\ 2m & \text{if } m \text{ is even,}\end{cases} \qquad \bar{n}_j = \begin{cases} n_j & \text{if } n_j \text{ is odd,}\\ 2n_j & \text{if } n_j \text{ is even.}\end{cases} \tag{B.2}$$

Let $\mathcal{H}^m$, $\mathcal{H}^{n_1}$, and $\mathcal{H}^{n_2}$ be Hilbert spaces with bases labelled by the elements in the rings $\mathbb{Z}_m$, $\mathbb{Z}_{n_1}$, and $\mathbb{Z}_{n_2}$, respectively. The assignment $|u\rangle \to |u_1\rangle\otimes|u_2\rangle$ defines an isometry from $\mathcal{H}^m$ onto $\mathcal{H}^{n_1}\otimes\mathcal{H}^{n_2}$. We use this isomorphism to identify $\mathcal{H}^m$ with $\mathcal{H}^{n_1}\otimes\mathcal{H}^{n_2}$. The displacement operators on $\mathcal{H}^m$ then split into pairs of displacement operators:

$$D^{(m)}_{a,b} = D^{(n_1)}_{a,\kappa_2 b} \otimes D^{(n_2)}_{a,\kappa_1 b}. \tag{B.3}$$

The integers κ_1 and κ_2 are the multiplicative inverses of n_1 and n_2 in arithmetic modulo $\bar{n}_2$ and $\bar{n}_1$, respectively. That is, $\kappa_1 n_1 = 1 \bmod \bar{n}_2$ and $\kappa_2 n_2 = 1 \bmod \bar{n}_1$. To verify (B.3), we calculate the action of the left-hand side operator on $|u\rangle$ and the action of the right-hand side operators on $|u_1\rangle$ and $|u_2\rangle$. The outcome is

$$D^{(m)}_{a,b}|u\rangle = \tau_m^{ab}\omega_m^{ub}|u+a\rangle, \tag{B.4}$$

$$D^{(n_1)}_{a,\kappa_2 b}|u_1\rangle = \tau_{n_1}^{ab\kappa_2}\omega_{n_1}^{u_1\kappa_2 b}|u_1+a_1\rangle, \tag{B.5}$$

$$D^{(n_2)}_{a,b\kappa_1}|u_2\rangle = \tau_{n_2}^{ab\kappa_1}\omega_{n_2}^{u_2 b\kappa_1}|u_2+a_2\rangle. \tag{B.6}$$

Since $|u+a\rangle = |u_1+a_1\rangle \otimes |u_2+a_2\rangle$, it suffices to prove that

$$\tau_m = \tau_{n_1}^{\kappa_2}\tau_{n_2}^{\kappa_1}, \tag{B.7}$$

$$\omega_m^u = \omega_{n_1}^{u_1\kappa_2}\omega_{n_2}^{u_2\kappa_1}. \tag{B.8}$$

To show that (B.7) holds, we first observe that $\bar{m} = \bar{n}_1\bar{n}_2$ and that $\bar{n}_1$ and $\bar{n}_2$ are relatively prime. For $j = 1, 2$ define

$$\nu_j = \begin{cases} \kappa_j & \text{if } n_j \text{ is odd,} \\ \frac{1}{2n_j}(m+n_j)\kappa_j & \text{if } n_j \text{ is even.} \end{cases} \tag{B.9}$$

The numbers ν_1 and ν_2 are the multiplicative inverses of $\bar{n}_1$ and $\bar{n}_2$ in arithmetic modulo $\bar{n}_2$ and $\bar{n}_1$, respectively, and $\nu_1\bar{n}_1 + \nu_2\bar{n}_2 = 1 \bmod \bar{m}$. Now, if n_1 and n_2 are both odd, then

$$\begin{aligned} \tau_m^{\nu_1\bar{n}_1+\nu_2\bar{n}_2} &= (-1)^{\nu_1\bar{n}_1+\nu_2\bar{n}_2}(\mathrm{e}^{\frac{\pi \mathrm{i}}{m}})^{\nu_1\bar{n}_1+\nu_2\bar{n}_2} \\ &= (-1)^{\kappa_1+\kappa_2}(\mathrm{e}^{\frac{\pi \mathrm{i}}{n_2}})^{\kappa_1}(\mathrm{e}^{\frac{\pi \mathrm{i}}{n_1}})^{\kappa_2} \\ &= \tau_{n_1}^{\kappa_2}\tau_{n_2}^{\kappa_1}, \end{aligned} \tag{B.10}$$

and if one of n_1 or n_2 is even, e.g. if n_1 is even and n_2 is odd, then

$$\begin{aligned} \tau_m^{\nu_1\bar{n}_1+\nu_2\bar{n}_2} &= (-1)^{\nu_1\bar{n}_1+\nu_2\bar{n}_2}(\mathrm{e}^{\frac{\pi \mathrm{i}}{m}})^{\nu_1\bar{n}_1+\nu_2\bar{n}_2} \\ &= (-1)^{\kappa_2}(\mathrm{e}^{\frac{\pi \mathrm{i}}{m}})^{2\nu_1 n_1}(\mathrm{e}^{\frac{\pi \mathrm{i}}{n_1}})^{\kappa_2} \\ &= \tau_{n_1}^{\kappa_2}(\mathrm{e}^{\frac{\pi \mathrm{i}}{n_2}})^{(n_2+1)\kappa_1} \\ &= \tau_{n_1}^{\kappa_2}\tau_{n_2}^{\kappa_1}. \end{aligned} \tag{B.11}$$

This proves (B.7). To prove (B.8), we use the result in (B.7) and calculate

$$\omega_m^u = \tau_m^{2u} = \tau_{n_1}^{2u\kappa_2}\tau_{n_2}^{2u\kappa_1} = \omega_{n_1}^{u\kappa_2}\omega_{n_2}^{u\kappa_1} = \omega_{n_1}^{u_1\kappa_2}\omega_{n_2}^{u_2\kappa_1}. \tag{B.12}$$

The last identity follows from $u\kappa_2 = u_1\kappa_2 \bmod n_1$ and $u\kappa_1 = u_2\kappa_1 \bmod n_2$.

Appendix C. Expansions of Π_1 and Π_2

In this appendix we derive the expansion (28) of Π_1 in the displacement operator basis. (The derivation of the expansion of Π_2 is similar so we omit it.) Starting from equation (19),

$$\begin{aligned}\Pi_1 &= \frac{d-1}{2d}\sum_{a,b=0}^{d-1} D^{(n)}_{(d-2)a,(d-2)b}|\psi_{0,0}\rangle\langle\psi_{0,0}|D^{(n)}_{(2-d)a,(2-d)b}\\ &= \frac{d-1}{2dn}\sum_{k,l=0}^{n^2-1}\sum_{a,b=0}^{d-1}\langle\psi_{0,0}|D^{(n)}_{k,l}|\psi_{0,0}\rangle D^{(n)}_{(d-2)a,(d-2)b}D^{(n)}_{-k,-l}D^{(n)}_{(2-d)a,(2-d)b}\\ &= \frac{d-1}{2dn}\sum_{k,l=0}^{n^2-1}\sum_{a,b=0}^{d-1}\langle\psi_{0,0}|D^{(n)}_{k,l}|\psi_{0,0}\rangle D^{(n)}_{-k,-l}\omega_n^{(d-2)(lb-ka)}\\ &= \frac{d-1}{2dn}\sum_{k,l=0}^{n^2-1}\sum_{a,b=0}^{d-1}\langle\psi_{0,0}|D^{(n)}_{k,l}|\psi_{0,0}\rangle D^{(n)}_{-k,-l}\omega_d^{la-kb}. \end{aligned} \tag{C.1}$$

In the second identity, we have inserted the expansion of $|\psi_{0,0}\rangle\langle\psi_{0,0}|$ in the displacement operator basis. In the third identity, we have used the commutation rule (7). Using that, for integer m,

$$\sum_{a=0}^{d-1}\omega_d^{ma} = d\delta^{(d)}_{0,m}, \tag{C.2}$$

we can proceed and write

$$\begin{aligned}\Pi_1 &= \frac{d(d-1)}{2n}\sum_{k,l=0}^{n^2-1}\langle\psi_{0,0}|D^{(n)}_{k,l}|\psi_{0,0}\rangle D^{(n)}_{-k,-l}\delta^{(d)}_{0,l}\,\delta^{(d)}_{0,k}\\ &= \frac{d(d-1)}{2n}\sum_{a,b=0}^{d-3}\langle\psi_{0,0}|D^{(n)}_{da,db}|\psi_{0,0}\rangle D^{(n)}_{-da,-db}. \end{aligned} \tag{C.3}$$

This is the expansion in equation (28).

Appendix D. Parity operators

In this appendix, we show that the Clifford group contains only two parity operators, namely $\pm P^{(n)}$ defined in equation (39). To this end, let P be any parity operator. In [19] it is shown that P, being a member of the Clifford group, can be decomposed as $P = \mathrm{e}^{\mathrm{i}\theta}D^{(n)}_{k,l}V_F$. Here, F is a matrix in $\mathrm{SL}(2,\mathbb{Z}_{\bar{n}})$ and V_F is the representation of F defined in section 2.1.3.

Suppose that

$$F = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}. \tag{D.1}$$

Since P is Hermitian, being an involution and a unitary,

$$\mathbb{1} = D^{(n)}_{k,l}V_F D^{(n)}_{1,0}V_F^\dagger D^{(n)}_{-k,-l}D^{(n)}_{1,0} = \omega_n^{-l}D^{(n)}_{k,l}D^{(n)}_{\alpha,\gamma}D^{(n)}_{1,0}D^{(n)}_{-k,-l} = \tau_n^{\gamma-2l}D^{(n)}_{k,l}D^{(n)}_{\alpha+1,\gamma}D^{(n)}_{-k,-l}. \tag{D.2}$$

The second identity follows from (13) and (7) and the third follows from (6). Similarly,

$$\mathbb{1} = D^{(n)}_{k,l}V_F D^{(n)}_{0,1}V_F^\dagger D^{(n)}_{-k,-l}D^{(n)}_{0,1} = \omega_n^{k}D^{(n)}_{k,l}D^{(n)}_{\beta,\delta}D^{(n)}_{1,0}D^{(n)}_{-k,-l} = \tau_n^{2k-\beta}D^{(n)}_{k,l}D^{(n)}_{\beta,\delta+1}D^{(n)}_{-k,-l}. \tag{D.3}$$

These two calculations, together with the requirement that $\alpha\delta - \beta\gamma = 1 \bmod \bar{n}$, show that if n is odd, then

Table D1. The possible values for the entries of F and the indices k, l of the displacement operator in the decomposition of P when n is even.

α	β	γ	δ	k	l
$-1 \bmod \bar{n}$	$0 \bmod \bar{n}$	$0 \bmod \bar{n}$	$-1 \bmod \bar{n}$	$0 \bmod n$	$0 \bmod n$
$-1 \bmod \bar{n}$	$0 \bmod \bar{n}$	$n \bmod \bar{n}$	$-1 \bmod \bar{n}$	$0 \bmod n$	$n/2 \bmod n$
$-1 \bmod \bar{n}$	$n \bmod \bar{n}$	$0 \bmod \bar{n}$	$-1 \bmod \bar{n}$	$n/2 \bmod n$	$0 \bmod n$
$-1 \bmod \bar{n}$	$n \bmod \bar{n}$	$n \bmod \bar{n}$	$-1 \bmod \bar{n}$	$n/2 \bmod n$	$n/2 \bmod n$
$n-1 \bmod \bar{n}$	$0 \bmod \bar{n}$	$0 \bmod \bar{n}$	$n-1 \bmod \bar{n}$	$0 \bmod n$	$0 \bmod n$
$n-1 \bmod \bar{n}$	$0 \bmod \bar{n}$	$n \bmod \bar{n}$	$n-1 \bmod \bar{n}$	$0 \bmod n$	$n/2 \bmod n$
$n-1 \bmod \bar{n}$	$n \bmod \bar{n}$	$0 \bmod \bar{n}$	$n-1 \bmod \bar{n}$	$n/2 \bmod n$	$0 \bmod n$
$n-1 \bmod \bar{n}$	$n \bmod \bar{n}$	$n \bmod \bar{n}$	$n-1 \bmod \bar{n}$	$n/2 \bmod n$	$n/2 \bmod n$

$$\alpha + 1 = \beta = \gamma = \delta + 1 = k = l = 0 \bmod n, \tag{D.4}$$

while if n is even, the multiple possible combinations for the entries of F and the indices k and l are the ones displayed in table D1. (If n is even, there is more than one option for the displacement operator in the fourth and eighth cases. But the different displacement operators differ only by a sign which can be included in the phase factor $\mathrm{e}^{\mathrm{i}\theta}$.)

First, assume that n is odd. According to (D.4), $P = \mathrm{e}^{\mathrm{i}\theta} V_F$ where

$$F = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = F_1 F_2. \tag{D.5}$$

By equations (12), (11), and (C.2),

$$V_F = \frac{1}{n} \sum_{u,v=0}^{n-1} \sum_{r,s=0}^{n-1} \omega_n^{uv+rs} |u\rangle\langle v|r\rangle\langle s| = \frac{1}{n} \sum_{u,s=0}^{n-1} \left(\sum_{v=0}^{n-1} \omega_n^{v(u+s)} \right) |u\rangle\langle s| = P^{(n)}, \tag{D.6}$$

and the assumption $P^2 = \mathbb{1}$ then forces the phase factor $\mathrm{e}^{\mathrm{i}\theta}$ to be ± 1. We conclude that $P = \pm P^{(n)}$.

Next, assume that n is even. Then, by table D1, there are eight cases to check. One can show that in all cases, $P = \pm P^{(n)}$. Since the arguments are similar in all cases, we will do only one of the calculations, say, when

$$\alpha = \delta = -1 \bmod \bar{n}, \qquad \beta = \gamma = n \bmod \bar{n}, \qquad k = l = n/2 \bmod n. \tag{D.7}$$

This is the fourth row in table D1. The decomposition

$$F = \begin{pmatrix} -1 & n \\ n & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} n & -1 \\ 1 & -n \end{pmatrix} = F_1 F_2 \tag{D.8}$$

is a prime decomposition of F and, hence, by (12) and (11),

$$V_F = \frac{1}{n} \sum_{u,v=0}^{n-1} \sum_{r,s=0}^{n-1} \omega_n^{uv} \tau_n^{-(ns^2 - 2rs - nr^2)} |u\rangle\langle v|r\rangle\langle s| = \frac{1}{n} \sum_{u,v,s=0}^{n-1} \tau_n^{n(v^2-s^2)} \omega_n^{v(u+s)} |u\rangle\langle s|. \tag{D.9}$$

Using that

$$\tau_n^{n(v^2-s^2)} = (-1)^{(v-s)} \tag{D.10}$$

and

$$\sum_{v=0}^{n-1}(-1)^v\omega_n^{v(u+s)} = n\delta^{(n)}_{u+s,n/2}, \tag{D.11}$$

we can further reduce the expression for V_F:

$$V_F = \frac{1}{n}\sum_{u,s=0}^{n-1}(-1)^s\left(\sum_{v=0}^{n-1}(-1)^v\omega_n^{v(u+s)}\right)|u\rangle\langle s| = \sum_{s=0}^{n-1}(-1)^s|n/2-s\rangle\langle s|. \tag{D.12}$$

Also, the displacement operator in the decomposition of P is

$$D^{(n)}_{n/2,n/2} = \tau_n^{n^2/4}X^{n/2}Z^{n/2} = i^{n/2}X^{n/2}Z^{n/2}. \tag{D.13}$$

If we post-compose V_F by this displacement operator, we obtain

$$\begin{aligned} D^{(n)}_{n/2,n/2}V_F &= i^{n/2}\sum_{s=0}^{n-1}(-1)^sX^{n/2}Z^{n/2}|n/2-s\rangle\langle s| \\ &= i^{n/2}\sum_{s=0}^{n-1}(-1)^s\omega_n^{n^2/4-sn/2}|-s\rangle\langle s| \\ &= (-i)^{n/2}P^{(n)}. \end{aligned} \tag{D.14}$$

Then, finally, for $P = \mathrm{e}^{\mathrm{i}\theta}D^{(n)}_{n/2,n/2}V_F$ to be an involution, the phase factor $\mathrm{e}^{\mathrm{i}\theta}$ must be such that $(-i)^{n/2}\mathrm{e}^{\mathrm{i}\theta} = \pm 1$. This finishes the proof that there is essentially only one parity operator, namely $P^{(n)}$, regardless of the parity of n.

Appendix E. Partial trace and local displacement operators

In this appendix, we prove equations (36) and (37).

Let $D^{(n_1)}_{a,b}$ and $D^{(n_2)}_{a,b}$ be the displacement operators corresponding to irreducible representations of $\mathrm{WH}(n_1)$ and $\mathrm{WH}(n_2)$ on an n_1-dimensional and an n_2-dimensional Hilbert space, respectively. Then, for any operator A on the composite Hilbert space,

$$\mathbb{1}_{n_1}\otimes \mathrm{tr}_{n_1}A = \frac{1}{n_1}\sum_{a,b=0}^{n_1-1}(D^{(n_1)}_{-a,b}\otimes\mathbb{1}_{n_2})A(D^{(n_1)}_{a,-b}\otimes\mathbb{1}_{n_2}), \tag{E.1}$$

$$\mathrm{tr}_{n_2}A\otimes\mathbb{1}_{n_2} = \frac{1}{n_2}\sum_{a,b=0}^{n_2-1}(\mathbb{1}_{n_1}\otimes D^{(n_2)}_{a,b})A(\mathbb{1}_{n_1}\otimes D^{(n_2)}_{-a,-b}). \tag{E.2}$$

Before we prove equation (E.1) (the proof of (E.2) is similar) we first prove that for any operator B on the first factor,

$$\frac{1}{n_1}\sum_{a,b=0}^{n_1-1}D^{(n_1)}_{-a,b}BD^{(n_1)}_{a,-b} = \mathrm{tr}B. \tag{E.3}$$

We expand B in the local displacement basis and use the commutation rule (7) to conclude that

$$\frac{1}{n_1}\sum_{a,b=0}^{n_1-1}D^{(n_1)}_{-a,b}BD^{(n_1)}_{a,-b} = \frac{1}{n_1^2}\sum_{k,l=0}^{n_1-1}\sum_{a,b=0}^{n_1-1}\mathrm{tr}(D^{(n_1)}_{k,l}B)\omega_{n_1}^{-bk-al}D^{(n_1)}_{-k,-l}. \tag{E.4}$$

Equation (E.3) now follows from the geometric sum (C.2).

Next we prove equation (E.1). We begin by expanding A in a product basis

$$A = \sum_{k,k'=0}^{n_1-1} \sum_{l,l'=0}^{n_2-1} A_{k,k';l,l'} |k\rangle\langle k'| \otimes |l\rangle\langle l'|. \tag{E.5}$$

If we then insert this expansion into the right-hand side of (E.1) and apply (E.3), the right-hand side reduces to

$$\begin{aligned} \frac{1}{n_1} \sum_{a,b=0}^{n_1-1} \sum_{k,k'=0}^{n_1-1} \sum_{l,l'=0}^{n_2-1} A_{k,k';l,l'} D^{(n_1)}_{-a,b} |k\rangle\langle k'| D^{(n_1)}_{a,-b} \otimes |l\rangle\langle l'| \\ = \sum_{k=0}^{n_1-1} \sum_{l,l'=0}^{n_2-1} A_{k,k;l,l'} \mathbb{1}_{n_1} \otimes |l\rangle\langle l'| = \mathbb{1}_{n_1} \otimes \mathrm{tr}_{n_1} A. \end{aligned} \tag{E.6}$$

This proves (E.1), from which equation (36) follows immediately. Equation (37) follows from (E.2).

ORCID iDs

Irina Dumitru https://orcid.org/0000-0002-1583-5866

References

[1] Renes J M, Blume-Kohout R, Scott A J and Caves C M 2004 Symmetric informationally complete quantum measurements *J. Math. Phys.* **45** 2171
[2] Scott A J 2006 Tight informationally complete quantum measurements *J. Phys. A: Math. Gen.* **39** 13507
[3] Zauner G 1999 Quantendesigns. Grundzüge einer nichtkommutativen Designtheorie *PhD Thesis* Univ. Wien
Zauner G 2011 *Int. J. Quantum Inf.* **9** 445 (Engl. transl.)
[4] Scott A J and Grassl M 2010 Symmetric informationally complete positive-operator valued measures: a new computer study *J. Math. Phys.* **51** 042203
[5] Grassl M and Scott A J private communication
[6] Appleby M, Flammia S, McConnell G and Yard J 2016 Generating ray class fields of real quadratic fields via complex equiangular lines (arXiv:1604.06098)
[7] Appleby M, Bengtsson I, Dumitru I and Flammia S 2017 Dimension towers of SICs. I. Aligned SICs and embedded tight frames *J. Math. Phys.* **58** 112201
[8] Grassl M and Scott A J 2017 Fibonacci-Lucas SIC-POVMs *J. Math. Phys.* **58** 122201
[9] Waldron S 2017 A sharpening of the Welch bounds and the existence of real and complex spherical *t*-designs *IEEE Trans. Inf. Theory* **63** 6849
[10] Appleby M, Bengtsson I, Flammia S and Goyeneche D 2019 Tight frames, Hadamard matrices and Zauner's conjecture *J. Phys. A: Math. Theor.* **52** 295301
[11] Appleby D M, Bengtsson I, Brierley S, Grassl M, Gross D and Larsson J-Å 2012 The monomial representations of the Clifford group *Quantum Inf. Comput.* **12** 044012
[12] Royer A 1977 Wigner function as the expectation value of a parity operator *Phys. Rev.* A **15** 449
[13] Gross D 2006 Hudson's theorem for finite-dimensional quantum systems *J. Math. Phys.* **47** 122107
[14] Chaturvedi S, Mukunda N and Simon R 2010 Wigner distributions for finite-state systems without redundant phase-point operators *J. Phys. A: Math. Theor.* **43** 075302
[15] Muñoz Villegas C A, Chavez Chavez A, Chumakov S, Fofanov Yu and Klimov A B 2003 On discrete quasiprobability distributions (arXiv:quant-ph/0307051)
[16] Benedetto J J and Fickus M 2003 Finite normalized tight frames *Adv. Comput. Math.* **18** 357–85

[17] Fuchs C A, Hoang M C and Stacey B C 2017 The SIC question: history and state of play *Axioms* **6** 21
[18] Weyl H 1930 *The Theory of Groups and Quantum Mechanics* (New York: Dover) (English translation of the 2nd edn)
[19] Appleby D M 2005 Symmetric informationally complete positive-operator valued measures and the extended Clifford group *J. Math. Phys.* **46** 052107
[20] McConnell G unpublished notes
[21] Ekert A and Knight P L 1995 Entangled quantum systems and the Schmidt decomposition *Am. J. Phys.* **63** 415
[22] Scott A J 2017 SICs: extending the list of solutions (arXiv:1703.03993)
[23] Appleby D M, Bengtsson I, Brierley S, Ericsson Å, Grassl M and Larsson J-Å 2014 Systems of imprimitivity for the Clifford group *Quantum Inf. Comput.* **14** 0339
[24] Appleby M unpublished notes

Paper III

Self-testing properties of Gisin's elegant Bell inequality

Ole Andersson,[*] Piotr Badziąg,[†] Ingemar Bengtsson,[‡] and Irina Dumitru[§]
Fysikum, Stockholms Universitet, 106 91 Stockholm, Sweden

Adán Cabello[‖]
Departamento de Física Aplicada II, Universidad de Sevilla, 41012 Sevilla, Spain
(Received 26 July 2017; published 22 September 2017)

An experiment in which the Clauser-Horne-Shimony-Holt inequality is maximally violated is self-testing (i.e., it certifies in a device-independent way both the state and the measurements). We prove that an experiment maximally violating Gisin's elegant Bell inequality is not similarly self-testing. The reason can be traced back to the problem of distinguishing an operator from its complex conjugate. We provide a complete and explicit characterization of all scenarios in which the elegant Bell inequality is maximally violated. This enables us to see exactly how the problem plays out.

DOI: 10.1103/PhysRevA.96.032119

I. INTRODUCTION

Bell inequalities are correlation inequalities which are satisfied by any local realistic model but can be violated by quantum theory [1]. They thus allow us to test the former against the latter. They are also useful in practical applications like secure communication [2], reduction of communication complexity [3], and secure private randomness [4]. For such applications, the self-testing properties of some Bell inequalities play a major role, as they allow a maximal quantum violation to occur in an effectively unique way. In the current paper we investigate the self-testing properties implied by a maximal violation of the so-called elegant Bell inequality (EBI).

The EBI involves two parties, Alice and Bob, measuring three and four dichotomic observables, respectively. If the possible outcomes of these observables are taken to be -1 and $+1$, and we write E_{kl} for the expectation value of the product of the outcomes of Alice's kth observable and Bob's lth observable, the EBI reads

$$S \equiv E_{11} + E_{12} - E_{13} - E_{14} + E_{21} - E_{22} + E_{23} - E_{24} + E_{31} - E_{32} - E_{33} + E_{34} \leqslant 6. \quad (1)$$

The EBI does not define a facet of the classical correlation polytope and, therefore, it does not reflect the geometry of the latter. Rather, according to Gisin [5], its elegance resides in the way it is maximally violated by quantum theory. The maximum violation, proven to be $S = 4\sqrt{3}$ by Acín *et al.* [6], occurs when Alice and Bob use projective measurements whose eigenstates are maximally spread out on Bloch spheres, in a sense made precise below. In the particular case when they share a two-qubit state, Alice's measurement eigenstates form a complete set of three mutually unbiased bases (MUBs), while those of Bob are eight states that can be partitioned into two dual sets of SIC elements, see Fig. 1. SICs are also known as symmetric informationally complete positive operator-valued measures (SIC-POVMs). However, here the configuration arises from four projective measurements and not from two POVMs. Since MUBs (and SICs) are intriguing configurations of independent interest [7], we can ask the question: does maximum quantum violation of the EBI *require* the existence of three MUBs in dimension two, with no assumptions about the preparation and measurement devices being made?

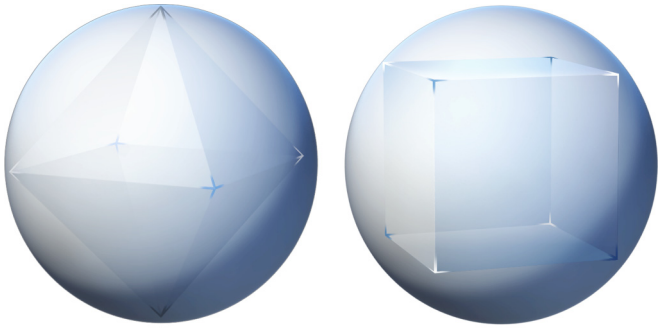
There is another motivation of more immediate practical relevance. Recently, Acín *et al.* [6] addressed the problem of how to use a two-qubit entangled state together with a local POVM measurement to certify the generation of two bits of device-independent private randomness. They provided two methods for such a certification. The simplest one was based on the EBI and was supported by numerical results. They suggested that an analytical proof of the correctness of the method should rely on a proof that a maximal violation of the EBI self-tests the maximally entangled state and the three Pauli measurements that give rise to the MUB.

In this paper we will prove that the EBI does *not* provide a self-test for the maximally entangled state and the three Pauli measurements, in the strict sense of Refs. [8,9]. It comes close to doing so though and we discuss the implications for the method suggested by Acín *et al.* in a separate paper [10]. In Sec. II of this paper we review the strict definition of self-testing. In Sec. III we discuss, following Refs. [6,11], maximal violation of the EBI. Section IV contains our main results on the self-testing properties of the EBI. To make the paper easier to read some of the detailed derivations are given in Sec. V. Finally, Sec. VI states our conclusions and the outlook.

II. SELF-TESTING EXPERIMENTS

The concept of *self-testing* was introduced by Mayers and Yao [12] as a test for a photon source which, if passed, guarantees that the source is adequate for the security of the BB84 protocol for quantum key distribution. Self-testing then received a stringent definition by the same authors in Ref. [13], a definition which was further polished by Magniez *et al.* [14] and McKague and Mosca [8,9]. In this paper we adopt the definition of self-testing used in these latter references.

[*]ole.andersson@fysik.su.se
[†]piotr.badziag@gmail.com
[‡]ingemar.bengtsson@fysik.su.se
[§]irina.dumitru@fysik.su.se
[‖]adan@us.es



(a) The octahedron in Alice's Bloch sphere. (b) The cube in Bob's Bloch sphere.

FIG. 1. Alice's and Bob's measurement eigenstates form two dual Platonic solids inscribed in Bloch spheres. Alice's eigenstates sit at the corners of an octahedron, Bob's eigenstates can be grouped into two dual sets of SIC vectors which sit at the corners of a cube. (a) The octahedron in Alice's Bloch sphere. (b) The cube in Bob's Bloch sphere.

The definition of being self-testing consists of a condensed description of how a *reference experiment* can be modified without affecting the statistics. Allowed modifications include local rotations, addition of ancillas, changes of the effect of observables outside the support of the state, and local embeddings of states and observables into greater or smaller Hilbert spaces [8,9]. Here we give the definition at a level of generality sufficient for our purposes. We thus consider a reference experiment involving two parties, Alice and Bob, performing m and n local dichotomic measurements $a_k = \{\Pi_\pm^{a_k}\}$ and $b_l = \{\Pi_\pm^{b_l}\}$, respectively, on a given bipartite state $|\phi\rangle$. (The subscript signs label the measurement outcomes.) We then say that the reference experiment is *self-testing* if for any other experiment in which Alice performs m local measurements $A_k = \{\Pi_\pm^{A_k}\}$ and Bob performs n local measurements $B_l = \{\Pi_\pm^{B_l}\}$ on a shared state $|\psi\rangle$, a complete agreement of the two experiments statistics, i.e., equality

$$\langle\phi|\Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi\rangle = \langle\psi|\Pi_\pm^{A_k}\Pi_\pm^{B_l}|\psi\rangle \tag{2}$$

for all k,l, implies the existence of a local unitary or, more precisely, a local isometric embedding

$$\begin{aligned}\Phi = \Phi_A \otimes \Phi_B : \mathcal{H}_A \otimes \mathcal{H}_B &\to (\mathcal{H}_A \otimes \mathcal{H}_a) \otimes (\mathcal{H}_B \otimes \mathcal{H}_b) \\ &= (\mathcal{H}_A \otimes \mathcal{H}_B) \otimes (\mathcal{H}_a \otimes \mathcal{H}_b)\end{aligned} \tag{3}$$

such that $\Phi(\Pi_\pm^{A_k}\Pi_\pm^{B_l}|\psi\rangle) = |\chi\rangle \otimes \Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi\rangle$, where $|\chi\rangle$ is some arbitrary but normalized "junk" vector in $\mathcal{H}_A \otimes \mathcal{H}_B$. (Here we use vocabulary introduced in Refs. [8,9].) Notice that the definition of self-testing captures, although in a rather abstract way, the physical intuition that the state generation includes a successful isolation of a "relevant part" of the total state. On this part, the measurements then act in a way stipulated by the reference experiment without entangling it with the rest of the state. We emphasize this by saying, for short, that the experiment is *effectively equivalent* to the reference experiment.

III. MAXIMAL VIOLATION OF THE EBI

The elegant Bell inequality can be violated in quantum theory. In fact, Acín *et al.* [6] have recently proven that the maximum quantum value that S can attain is $4\sqrt{3}$. The simplest setting when this happens, it turns out, is when Alice and Bob share two qubits in the maximally entangled state

$$|\phi_+\rangle = \tfrac{1}{\sqrt{2}}(|0_a 0_b\rangle + |1_a 1_b\rangle), \tag{4}$$

Alice's observables correspond to the three Pauli operators

$$a_1 = Z = \sigma_Z, \quad a_2 = X = \sigma_X, \quad a_3 = Y = \sigma_Y, \tag{5}$$

and Bob's observables correspond to

$$b_1 = \tfrac{1}{\sqrt{3}}(Z + X - Y), \quad b_3 = \tfrac{1}{\sqrt{3}}(-Z + X + Y), \tag{6a}$$

$$b_2 = \tfrac{1}{\sqrt{3}}(Z - X + Y), \quad b_4 = \tfrac{1}{\sqrt{3}}(-Z - X - Y). \tag{6b}$$

The elegance of the Bell inequality (1) is apparent [5] when we observe that the observables in Eqs. (5) and (6) give rise to two measurement structures which can be represented by two dual polyhedra in the Bloch ball: Alice's measurement eigenstates form a complete set of three MUBs, with each basis corresponding to a pair of opposite corners of an octahedron inscribed in the Bloch sphere, see Fig. 1(a). On the Bloch sphere, the eight eigenstates of Bob's projective measurements form the vertices of a dual cube, see Fig. 1(b). They can be grouped into two tetrahedra containing no adjacent corners. The vertices of such a tetrahedron can be regarded as the four vectors in a SIC, and we can arrange them such that one SIC is formed by the -1 outcome projectors and the other by the $+1$ outcome projectors. Below we will show that, in general, the EBI is maximally violated if and only if the state is a superposition of maximally entangled qubit states like the one in Eq. (4) and Alice's and Bob's observables split into direct sums of qubit MUB-SIC configurations similar to that just described.

To characterize all scenarios in which the EBI is maximally violated we consider a general one in which Alice measures three dichotomic observables A_1, A_2, A_3 and Bob measures four dichotomic observables B_1, B_2, B_3, B_4, all of which take the values -1 or $+1$, on a bipartite system in a state $|\psi\rangle$ such that $\langle\psi|\Sigma|\psi\rangle = 4\sqrt{3}$, where Σ is the *elegant Bell operator*:

$$\begin{aligned}\Sigma \equiv\ & A_1B_1 + A_1B_2 - A_1B_3 - A_1B_4 + A_2B_1 - A_2B_2 \\ & + A_2B_3 - A_2B_4 + A_3B_1 - A_3B_2 - A_3B_3 + A_3B_4.\end{aligned} \tag{7}$$

The first assertion, which, like all other assertions in this section, is proven in Sec. V, is that Alice's and Bob's observables preserve the supports, even the eigenspaces, of the respective marginal states: If $\lambda_1, \lambda_2, \ldots, \lambda_m$ are the *different* Schmidt coefficients of $|\psi\rangle$, having multiplicities $d_1, d_2, \ldots, d_m$, and $\mathcal{H}_A^i$ and $\mathcal{H}_B^i$ denote the d_i-dimensional eigenspaces of $\mathrm{tr}_B\,|\psi\rangle\langle\psi|$ and $\mathrm{tr}_A\,|\psi\rangle\langle\psi|$ corresponding to the eigenvalue λ_i^2, then Alice's observables send $\mathcal{H}_A^i$ into itself and Bob's observables send $\mathcal{H}_B^i$ into itself. As a consequence we can, without loss of generality, truncate Alice's and Bob's Hilbert spaces and restrict the observables to the support of the respective marginal state. We henceforth assume this has been done and we write A_k^i and B_l^i for the restriction of Alice's kth and Bob's lth observable to $\mathcal{H}_A^i$ and $\mathcal{H}_B^i$, respectively.

The second assertion is that Alice's observables anticommute: $\{A_k, A_l\} = 2\delta_{kl}$. (Since their eigenvalues equal -1 or $+1$, Alice's and Bob's observables are involutions, i.e., they square to the identity operator.) From this follows that $\mathcal{H}_A^i$ is even-dimensional, say $d_i = 2n_i$, and can be split into 2-dimensional and pairwise orthogonal subspaces, each left invariant by Alice's observables:

$$\mathcal{H}_A^i = \bigoplus_{p=1}^{n_i} \mathcal{H}_A^{ip}, \quad A_k^i = \bigoplus_{p=1}^{n_i} A_k^{ip}. \tag{8}$$

Furthermore, each subspace $\mathcal{H}_A^{ip}$ admits a basis $\{|0_A^{ip}\rangle, |1_A^{ip}\rangle\}$ with respect to which

$$A_1^{ip} = Z, \quad A_2^{ip} = X, \quad A_3^{ip} = \pm Y. \tag{9}$$

Notice the indefinite sign of A_3^{ip}; a similar sign indeterminacy was identified in [8], treating a related problem.

The third assertion is that every $\mathcal{H}_B^i$ can as well be decomposed into 2-dimensional orthogonal subspaces, each of which is left invariant by Bob's observables:

$$\mathcal{H}_B^i = \bigoplus_{p=1}^{n_i} \mathcal{H}_B^{ip}, \quad B_l^i = \bigoplus_{p=1}^{n_i} B_l^{ip}. \tag{10}$$

Moreover, $\mathcal{H}_B^{ip}$ admits a basis $\{|0_B^{ip}\rangle, |1_B^{ip}\rangle\}$ such that, as matrices with respect to $\{|0_A^{ip}\rangle, |1_A^{ip}\rangle\}$ and $\{|0_B^{ip}\rangle, |1_B^{ip}\rangle\}$,

$$B_1^{ip} = \tfrac{1}{\sqrt{3}}\left(A_1^{ip} + A_2^{ip} - A_3^{ip}\right) = \tfrac{1}{\sqrt{3}}(Z + X \mp Y), \tag{11a}$$

$$B_2^{ip} = \tfrac{1}{\sqrt{3}}\left(A_1^{ip} - A_2^{ip} + A_3^{ip}\right) = \tfrac{1}{\sqrt{3}}(Z - X \pm Y), \tag{11b}$$

$$B_3^{ip} = \tfrac{1}{\sqrt{3}}\left(-A_1^{ip} + A_2^{ip} + A_3^{ip}\right) = \tfrac{1}{\sqrt{3}}(-Z + X \pm Y), \tag{11c}$$

$$B_4^{ip} = \tfrac{1}{\sqrt{3}}\left(-A_1^{ip} - A_2^{ip} - A_3^{ip}\right) = \tfrac{1}{\sqrt{3}}(-Z - X \mp Y). \tag{11d}$$

The fourth and last assertion concerns the state. The bases $\{|0_A^{ip}\rangle, |1_A^{ip}\rangle\}$ and $\{|0_B^{ip}\rangle, |1_B^{ip}\rangle\}$ are eigenbases of Alice's and Bob's local states which will be constructed in such a way that the shared state obtains the representation

$$\begin{aligned} |\psi\rangle &= \sum_{i=1}^{m} \sum_{p=1}^{n_i} \lambda_i \left(|0_A^{ip} 0_B^{ip}\rangle + |1_A^{ip} 1_B^{ip}\rangle\right) \\ &= \sqrt{2} \sum_{i=1}^{m} \sum_{p=1}^{n_i} \lambda_i |\phi_+^{ip}\rangle. \end{aligned} \tag{12}$$

Notice that $|\phi_+^{ip}\rangle$ is the Einstein-Podolsky-Rosen singlet in the space $\mathcal{H}_A^{ip} \otimes \mathcal{H}_B^{ip}$, restricted to which Alice's and Bob's observables are given by Eqs. (9) and (11). For each i, we arrange that $A_3^{ip} = Y$ for $p \leqslant r_i$ and $A_3^{ip} = -Y$ for $p > r_i$, where $0 \leqslant r_i \leqslant n_i$. For any Schmidt coefficients λ_i and any r_i the EBI is maximally violated.

We end this section with some remarks about mixed states and general measurements violating the EBI maximally. If Alice and Bob share a mixed state which can be expanded as an incoherent sum of pure states, each of which individually maximally violates the EBI, then so does the mixed state. A straightforward convexity argument then shows that this is the only possibility for a mixed state violating the EBI maximally. One can also ask if the EBI can be maximally violated by nonprojective measurements. It turns out that this is not possible. More precisely, if Alice and Bob measure local dichotomic POVMs and the EBI is maximally violated, then the measurement operators preserve the supports of the local states, and when restricted to these supports the measurements are projective. A proof of this can be based on Naimark's dilation theorem (see, e.g., [15]) and the arguments in the second paragraph in Sec. V below.

IV. SELF-TESTING PROPERTIES OF THE EBI

By the previous section, Alice's observables split into an unknown number of 2-dimensional $\mathfrak{su}(2)$ representations and an unknown number of "transposed" $\mathfrak{su}(2)$ representations. The statistics, however, is independent of these numbers, since the statistics equals that of the experiment specified by Eqs. (4)–(6), from now on referred to as "the reference experiment." The reference experiment is therefore not self-testing, and neither is any other experiment in which only a maximal violation of the EBI is assumed. For if a local isometric embedding Φ exists, establishing an effective equivalence between the reference experiment and the generic experiment in Sec. III, then

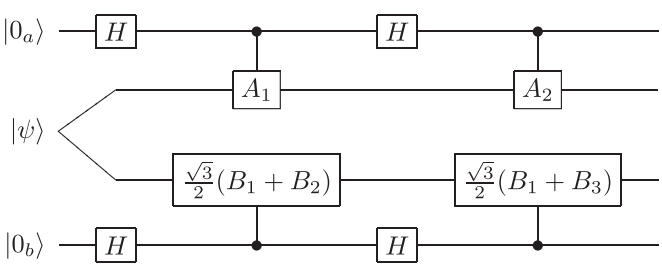
$$\begin{aligned} \langle \phi_+ | a_2 a_3 (b_1 + b_2) | \phi_+ \rangle &= \langle \Phi(A_2|\psi\rangle) | \Phi(A_3(B_1 + B_2)|\psi\rangle) \rangle \\ &= \langle \psi | A_2 A_3 (B_1 + B_2) | \psi \rangle. \end{aligned} \tag{13}$$

But $\langle \phi_+ | a_2 a_3 (b_1 + b_2) | \phi_+ \rangle = 2i/\sqrt{3}$ and

$$\langle \psi | A_2 A_3 (B_1 + B_2) | \psi \rangle = \frac{2i}{\sqrt{3}} \sum_{i=1}^{m} \lambda_i^2 (4r_i - 2n_i). \tag{14}$$

The results agree if and only if $r_i = n_i$ for all i. (Remember that $2n_i$ is the multiplicity of the Schmidt coefficient λ_i.) But, because the values of the differences $n_i - r_i$ are not determinable from the statistics of the experiment, this shows that a maximal violation of the EBI is not sufficient to conclude that the reference experiment is self-testing.

On the other hand, if we *require* that Eq. (13) *is* satisfied, in addition to a maximal violation of the EBI, the reference experiment *is* self-testing; an equivalence is provided by the local isometric embedding Φ given by the circuit



(Here H denotes the Hadamard gate and the control gates are triggered by the presence of $|1_a\rangle$ and $|1_b\rangle$.) McKague and Mosca used this isometric embedding to develop a generalized Mayers-Yao test, see [8], and McKague *et al.* [16] used it to show that the standard scenario in which the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality is maximally violated is robustly self-testing. Recently, a more universal form of this

isometric embedding was used to prove that all pure bipartite entangled states can be self-tested [17].

Straightforward calculations show that

$$\Phi\big(\Pi_\pm^{A_k}\Pi_\pm^{B_l}\big|\phi_+^{ip}\big)\big) = \big|0_A^{ip}0_B^{ip}\big\rangle \otimes \Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi_+\rangle, \tag{15}$$

where $\Pi_\pm^{A_k}$ and $\Pi_\pm^{B_l}$ are the projections onto the ±1 eigenspaces of A_k and B_l, and $\Pi_\pm^{a_k}$ and $\Pi_\pm^{b_l}$ are the projections onto the ±1 eigenspaces of the observables a_k and b_l in the reference experiment. Consequently,

$$\begin{aligned}\Phi\big(\Pi_\pm^{A_k}\Pi_\pm^{B_l}|\psi\rangle\big) &= \sqrt{2}\sum_{i=1}^{m}\sum_{p=1}^{n_i}\lambda_i\big|0_A^{ip}0_B^{ip}\big\rangle \otimes \Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi_+\rangle \\ &= |\chi\rangle \otimes \Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi_+\rangle. \end{aligned}\tag{16}$$

The last identity in Eq. (16) defines the junk vector $|\chi\rangle$. If Eq. (13) is *not* satisfied, the junk vector naturally splits into two parts, $|\chi\rangle = |\chi_1\rangle + |\chi_2\rangle$, defined by

$$|\chi_1\rangle = \sqrt{2}\sum_{i=1}^{m}\sum_{p=1}^{r_i}\lambda_i\big|0_A^{ip}0_B^{ip}\big\rangle, \tag{17}$$

$$|\chi_2\rangle = \sqrt{2}\sum_{i=1}^{m}\sum_{p=r_i+1}^{n_i}\lambda_i\big|0_A^{ip}0_B^{ip}\big\rangle. \tag{18}$$

Equation (16) is then no longer valid. Instead we have that

$$\Phi\big(\Pi_\pm^{A_1}\Pi_\pm^{B_l}|\psi\rangle\big) = |\chi_1\rangle\Pi_\pm^{a_1}\Pi_\pm^{b_l}|\phi_+\rangle + |\chi_2\rangle\Pi_\pm^{a_1}\Pi_\mp^{b_{5-l}}|\phi_+\rangle, \tag{19a}$$

$$\Phi\big(\Pi_\pm^{A_2}\Pi_\pm^{B_l}|\psi\rangle\big) = |\chi_1\rangle\Pi_\pm^{a_2}\Pi_\pm^{b_l}|\phi_+\rangle + |\chi_2\rangle\Pi_\pm^{a_2}\Pi_\mp^{b_{5-l}}|\phi_+\rangle, \tag{19b}$$

$$\Phi\big(\Pi_\pm^{A_3}\Pi_\pm^{B_l}|\psi\rangle\big) = |\chi_1\rangle\Pi_\pm^{a_3}\Pi_\pm^{b_l}|\phi_+\rangle + |\chi_2\rangle\Pi_\mp^{a_3}\Pi_\mp^{b_{5-l}}|\phi_+\rangle. \tag{19c}$$

Using these identities one can show that a measurement of Alice's third observable, or a measurement of any of Bob's observables, entangles the singlet part of the state with the junk part. But, interestingly, even though an adversary, Eve, having access only to the junk part, can detect a measurement of A_3 or any of the B_l, she cannot distinguish between the outcomes. This is so because, irrespective of the measurement outcome, all these measurements leave Eve's system in the same state.

V. DERIVATIONS

In this section we prove the assertions in Sec. III. Inspiration comes mainly from Acín *et al.*'s derivation of the least quantum bound for the EBI [6] and from Popescu and Rohrlich's characterization of the scenarios in which the CHSH Bell inequality is maximally violated [11].

First we prove that Alice's and Bob's observables preserve the supports of the marginal states. Thus let $|\psi\rangle$ be a state saturating the EBI and let $|\psi\rangle = \sum_{i=1}^{m}\sum_{p=1}^{d_i}\lambda_i|u_p^i v_p^i\rangle$ be a Schmidt decomposition, with i labeling the m different Schmidt coefficients and d_i being the multiplicity of λ_i. Define

$$D_1 = \tfrac{1}{\sqrt{3}}(A_1 + A_2 + A_3), \tag{20a}$$

$$D_2 = \tfrac{1}{\sqrt{3}}(A_1 - A_2 - A_3), \tag{20b}$$

$$D_3 = \tfrac{1}{\sqrt{3}}(-A_1 + A_2 - A_3), \tag{20c}$$

$$D_4 = \tfrac{1}{\sqrt{3}}(-A_1 - A_2 + A_3). \tag{20d}$$

Then $\sum_{l=1}^{4}(D_l - B_l)^2 = 8\mathbb{1} - 2\Sigma/\sqrt{3}$ and, hence,

$$\sum_{i=1}^{m}\sum_{p=1}^{d_i}\lambda_i D_l\big|u_p^i v_p^i\big\rangle = \sum_{i=1}^{m}\sum_{p=1}^{d_i}\lambda_i B_l\big|u_p^i v_p^i\big\rangle. \tag{21}$$

Multiplication of both sides by $\langle w, v_q^j|$, where $|w\rangle$ is any vector in $\mathcal{H}_A$ perpendicular to the support of $\mathrm{tr}_B|\psi\rangle\langle\psi|$, yields the identity $\lambda_j\langle w|D_l|u_q^j\rangle = 0$. Since the indices j and q are arbitrary and $\lambda_j > 0$, this proves that D_l preserves the support of $\mathrm{tr}_B|\psi\rangle\langle\psi|$. Then so does each A_k. A similar argument shows that the operators B_l preserve the support of the marginal state $\mathrm{tr}_A|\psi\rangle\langle\psi|$.

Next we prove that Alice's and Bob's observables preserve the eigenspaces of the marginal states. From Eq. (21) follows that for any two pairs of indices (i_1, p_1) and (i_2, p_2),

$$\lambda_{i_2}\big\langle u_{p_1}^{i_1}|D_l|u_{p_2}^{i_2}\big\rangle = \lambda_{i_1}\big\langle v_{p_2}^{i_2}|B_l|v_{p_1}^{i_1}\big\rangle. \tag{22}$$

This, in turn, implies that

$$\lambda_{i_1}^2\big\langle u_{p_1}^{i_1}|D_l|u_{p_2}^{i_2}\big\rangle = \lambda_{i_2}^2\big\langle u_{p_1}^{i_1}|D_l|u_{p_2}^{i_2}\big\rangle. \tag{23}$$

From Eq. (23) we can deduce that D_l and, hence, each A_k preserve the eigenspaces $\mathcal{H}_A^i$. By an identical argument also the operators B_l preserve the eigenspaces $\mathcal{H}_B^i$. We write A_k^i and D_l^i for the restrictions of A_k and D_l to $\mathcal{H}_A^i$, and B_l^i for the restriction of B_l to $\mathcal{H}_B^i$.

From Eq. (20) and the A_k being involutions follow that

$$\big(D_1^i\big)^2 = \mathbb{1} + \tfrac{1}{3}\big(\{A_1^i, A_2^i\} + \{A_1^i, A_3^i\} + \{A_2^i, A_3^i\}\big), \tag{24a}$$

$$\big(D_2^i\big)^2 = \mathbb{1} - \tfrac{1}{3}\big(\{A_1^i, A_2^i\} - \{A_1^i, A_3^i\} + \{A_2^i, A_3^i\}\big), \tag{24b}$$

$$\big(D_3^i\big)^2 = \mathbb{1} - \tfrac{1}{3}\big(\{A_1^i, A_2^i\} + \{A_1^i, A_3^i\} - \{A_2^i, A_3^i\}\big), \tag{24c}$$

$$\big(D_4^i\big)^2 = \mathbb{1} + \tfrac{1}{3}\big(\{A_1^i, A_2^i\} - \{A_1^i, A_3^i\} - \{A_2^i, A_3^i\}\big). \tag{24d}$$

Furthermore, from Eq. (22) and each B_l being an involution follows that D_l^i is an involution. But then, by Eq. (24),

$$\{A_1^i, A_2^i\} = \{A_1^i, A_3^i\} = \{A_2^i, A_3^i\} = 0. \tag{25}$$

Equation (25) implies that A_1^i, A_2^i, and $[A_1^i, A_2^i]/2i$ generate an $\mathfrak{su}(2)$ representation. We cannot, however, conclude that $A_3^i = [A_1^i, A_2^i]/2i$. Nevertheless, among the irreducible $\mathfrak{su}(2)$ representations only the 2-dimensional one satisfies Eq. (25). The space $\mathcal{H}_A^i$ must therefore be even-dimensional, say $d_i = 2n_i$, and be decomposable into an orthogonal direct sum of 2-dimensional subspaces, $\mathcal{H}_A^i = \bigoplus_{p=1}^{n_i}\mathcal{H}_A^{ip}$, each of which is left invariant by A_1^i and A_2^i; thus $A_1^i = \bigoplus_{p=1}^{n_i}A_1^{ip}$ and $A_2^i = \bigoplus_{p=1}^{n_i}A_2^{ip}$. Furthermore, since A_1^i and A_2^i are involutions, we can choose a provisional basis $\{|s_A^i\rangle\}_{s=1}^{d_i}$ in each $\mathcal{H}_A^i$ such that for every $1 \leqslant p \leqslant n_i$, $\{|(2p-1)_A^i\rangle, |(2p)_A^i\rangle\}$ is a basis in $\mathcal{H}_A^{ip}$ relative to which $A_1^{ip} = Z$ and $A_2^{ip} = X$.

It remains to prove that the decomposition of $\mathcal{H}_A^i$ can be chosen such that A_3^i also splits into a direct sum, $A_3^i = \bigoplus_{p=1}^{n_i}A_3^{ip}$, and that the basis in $\mathcal{H}_A^{ip}$ can be chosen such that $A_3^{ip} = \pm Y$. To this end, let $(A_3^i)_{p_2}^{p_1}$ be the 2×2 matrix

which in the provisional basis describes how A_3^i connects $\mathcal{H}_A^{ip_1}$ to $\mathcal{H}_A^{ip_2}$. Then, by Eq. (25), and since A_3^i is Hermitian, $(A_3^i)_{p_2}^{p_1} = \omega_{p_2}^{p_1} Y$ for some real number $\omega_{p_2}^{p_1}$. Next introduce a tensor product structure in $\mathcal{H}_A^i$ by writing $|(2p-1)_A^i\rangle = |p\rangle \otimes |0\rangle$ and $|(2p)_A^i\rangle = |p\rangle \otimes |1\rangle$. Then $A_1^i = \mathbb{1} \otimes Z$, $A_2^i = \mathbb{1} \otimes X$, and $A_3^i = \Omega \otimes Y$, where Ω is the $n_i \times n_i$ matrix whose element on position (p_1, p_2) is $\omega_{p_2}^{p_1}$. Being Hermitian, Ω can be diagonalized, say $U^\dagger \Omega U = \mathrm{diag}(\omega_1, \omega_2, \ldots, \omega_{n_i})$. Then

$$(U^\dagger \otimes \mathbb{1}) A_1^i (U \otimes \mathbb{1}) = \mathbb{1} \otimes Z, \tag{26a}$$

$$(U^\dagger \otimes \mathbb{1}) A_2^i (U \otimes \mathbb{1}) = \mathbb{1} \otimes X, \tag{26b}$$

$$(U^\dagger \otimes \mathbb{1}) A_3^i (U \otimes \mathbb{1}) = \mathrm{diag}(\omega_1, \omega_2, \ldots, \omega_{n_i}) \otimes Y. \tag{26c}$$

Each diagonal element ω_p equals $+1$ or -1 because A_3^i is an involution. We choose U such that $\omega_p = +1$ for $p \leqslant r_i$ and $\omega_p = -1$ for $p > r_i$, where r_i is the number of positive diagonal elements. We then rotate the provisional basis by applying $U^\dagger \otimes \mathbb{1}$ to it and rotate the $\mathcal{H}_A^{ip}$ accordingly.

Next we consider Bob's observables. These are completely determined by Alice's observables. To see this, define

$$|s_B^i\rangle = \sum_{p=1}^{n_i} |v_p^i\rangle \langle s_A^i | u_p^i \rangle. \tag{27}$$

Then $\langle s_B^i | B_l^i | t_B^i \rangle = \langle t_A^i | D_l^i | s_A^i \rangle$ and, hence, by Eq. (20),

$$B_1^i = \tfrac{1}{\sqrt{3}} \left(A_1^i + A_2^i + A_3^i \right)^T, \tag{28a}$$

$$B_2^i = \tfrac{1}{\sqrt{3}} \left(A_1^i - A_2^i - A_3^i \right)^T, \tag{28b}$$

$$B_3^i = \tfrac{1}{\sqrt{3}} \left(-A_1^i + A_2^i - A_3^i \right)^T, \tag{28c}$$

$$B_4^i = \tfrac{1}{\sqrt{3}} \left(-A_1^i - A_2^i + A_3^i \right)^T. \tag{28d}$$

This proves Eqs. (11).

The assertion about the state is a straightforward consequence of the calculation

$$\begin{aligned} |\psi\rangle &= \sum_{i=1}^{m} \sum_{p=1}^{d_i} \lambda_i |u_p^i v_p^i\rangle \\ &= \sum_{i=1}^{m} \sum_{p=1}^{d_i} \sum_{s=1}^{d_i} \sum_{t=1}^{d_i} \lambda_i |s_A^i t_B^i\rangle \langle s_A^i | u_p^i \rangle \langle t_B^i | v_p^i \rangle \\ &= \sum_{i=1}^{m} \sum_{s=1}^{d_i} \sum_{t=1}^{d_i} \lambda_i |s_A^i t_B^i\rangle \delta_{st} \\ &= \sum_{i=1}^{m} \sum_{p=1}^{n_i} \lambda_i \left(|(2p-1)_A^i (2p-1)_B^i\rangle + |(2p)_A^i (2p)_B^i\rangle \right). \end{aligned} \tag{29}$$

If we define

$$|0_A^{ip}\rangle = |(2p-1)_A^i\rangle, \quad |1_A^{ip}\rangle = |(2p)_A^i\rangle, \tag{30}$$

$$|0_B^{ip}\rangle = |(2p-1)_B^i\rangle, \quad |1_B^{ip}\rangle = |(2p)_B^i\rangle, \tag{31}$$

then $|\psi\rangle$ takes the form in Eq. (12).

VI. CONCLUDING REMARKS

We have shown that maximal violation of the EBI by itself does not certify self-testability; additional requirements need to be met. The extra requirement that Eq. (13) should also be satisfied makes the experiment self-testing. That a maximal violation of the EBI does not lead to self-testability is because transposition of *some* of the components of Alice's observables does not affect the statistics but leads to an *inequivalent* experiment. Similar issues have been pointed out by other authors, see, e.g., Refs. [8,18], and it has been suggested that the definition of self-testing should be relaxed "to include this transposition equivalence" [19]. Then the results in this paper have to be taken into account since in such a relaxation we may be losing physically relevant information, as Eq. (14) shows. Alternative approaches to self-testing based on quantification of incompatibility of measurements have been proposed [18,20].

In addition, we have completely and explicitly characterized the scenarios in which the EBI is maximally violated. For a pair of qubits, maximal violation requires measurements corresponding to mutually unbiased bases on the Bloch sphere on one side and to measurements along the diagonals of a dual cube (inscribed in the Bloch sphere) on the other. The general case is a superposition of that for the pair of qubits.

In many applications, Bell inequalities are used to guarantee that quantum mechanical systems exhibit desired properties. The present paper provides information about the EBI which is potentially useful in any situation where a maximal violation of the EBI is used as such a resource. Examples include a construction for device-independent generation of private randomness proposed by Acín *et al.* [6]. We discuss this construction in a companion paper [10].

ACKNOWLEDGMENTS

We thank M. Nawareg and M. Smania for fruitful discussions, J. Kaniewski and Y.-C. Liang for useful comments on an earlier draft of the paper, and N. Gisin for encouraging remarks. We also thank P. Z. Andersson who produced Fig. 1. A.C. acknowledges support from Project No. FIS2014-60843-P, "Advanced Quantum Information" (MINECO, Spain), with FEDER funds, the FQXi Large Grant "The Observer Observed: A Bayesian Route to the Reconstruction of Quantum Theory," and the project "Photonic Quantum Information" (Knut and Alice Wallenberg Foundation, Sweden).

[1] J. S. Bell, On the Einstein Podolsky Rosen paradox, Physics **1**, 195 (1964).

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, Bell's Inequalities and Quantum Communication Complexity, Phys. Rev. Lett. **92**, 127901 (2004).

[4] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2006, arXiv:0911.3814.

[5] N. Gisin, Bell inequalities: Many questions, a few answers, in *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony*, The Western Ontario Series in Philosophy of Science, edited by W. C. Myrvold and J. Christian (Springer, Berlin, 2009), Vol. 73, p. 125.

[6] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A **93**, 040102(R) (2016).

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

[8] M. McKague and M. Mosca, Generalized self-testing and the security of the 6-state protocol, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science, edited by W. van Dam, V. M. Kendon, and S. Severini (Springer, Berlin, 2010), Vol. 6519, p. 113.

[9] M. McKague, Quantum information processing with adversarial devices, Ph.D. thesis, University of Waterloo, 2010, arXiv:1006.2352.

[10] O. Andersson, P. Badziąg, I. Dumitru, and A. Cabello, Certification of two bits of randomness from one entangled bit using the elegant Bell inequality, arXiv:1707.00564.

[11] S. Popescu and D. Rohrlich, Which states violate Bell's inequality maximally?, Phys. Lett. A **169**, 411 (1992).

[12] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, in *Proceedings of the 39th IEEE Conference on Foundations of Computer Science, Palo Alto, CA, 1998*) (IEEE, New York, 1998).

[13] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inf. Comput. **4**, 273 (2004).

[14] F. Magniez, D. Mayers, M. Mosca, and H. Olliver, Self-testing of quantum circuits, in *Proceedings of ICALP 2006*, Part I, Lecture Notes in Computer Science, edited by M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener (Springer, Berlin, 2006), Vol. 4051, p. 72.

[15] A. Holevo, in *Probabilistic and Statistical Aspects of Quantum Theory* (Scuola Normale Superiore Pisa, Pisa, Italy, 2011), p. 55.

[16] M. McKague, T. H. Yang, and V. Scarani, Robust self-testing of the singlet, J. Phys. A **45**, 455304 (2012).

[17] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. **8**, 15485 (2017).

[18] J. Kaniewski, Self-testing of binary observables based on commutation, Phys. Rev. A **95**, 062323 (2017).

[19] J. Kaniewski (private communication).

[20] S.-L. Chen, C. Budroni, Y.-C. Liang, and Y.-N. Chen, Natural Framework for Device-Independent Quantification of Quantum Steerability, Measurement Incompatibility, and Self-Testing, Phys. Rev. Lett. **116**, 240401 (2016).

Paper IV

Device-independent certification of two bits of randomness from one entangled bit and Gisin's elegant Bell inequality

Ole Andersson,[*] Piotr Badziąg,[†] and Irina Dumitru[‡]
Fysikum, Stockholms Universitet, S-106 91 Stockholm, Sweden

Adán Cabello[§]
Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain

(Received 30 September 2017; published 16 January 2018)

We prove that as conjectured by Acín *et al.* [Phys. Rev. A **93**, 040102(R) (2016)], two bits of randomness can be certified in a device-independent way from one bit of entanglement using the maximal quantum violation of Gisin's elegant Bell inequality. This suggests a surprising connection between maximal entanglement, complete sets of mutually unbiased bases, and elements of symmetric informationally complete positive operator-valued measures, on one side, and the optimal way of certifying maximal randomness, on the other.

DOI: 10.1103/PhysRevA.97.012314

I. INTRODUCTION

Random numbers, i.e., numbers unpredictable to anyone, play a crucial role in cryptography, algorithms, and simulation. The possibility of certifying random numbers in a device-independent (DI) way, i.e., without making any assumption about the devices used to produce them and only assuming the impossibility of superluminal communication [1–3], is a great achievement of quantum information.

All methods for DI randomness certification [1–3] require entangled pairs of systems and spacelike separated measurements whose outcomes violate one or several Bell inequalities [4] and, therefore, cannot be produced by any local realistic mechanism. The fact that entanglement and Bell inequality violation are the fundamental ingredients for DI randomness certification immediately raises two questions: (i) How many random bits can be certified from one ebit? (The *ebit* is the unit of bipartite entanglement and is defined as the amount of entanglement contained in a maximally entangled two-qubit state [5].) (ii) Which is the simplest Bell inequality, i.e., the one with the smallest number of settings, which allows for the DI certification of the maximal number of random bits? Question (i) has been answered recently. D'Ariano *et al.* [6] have proven that the maximum number of bits that can be certified in a DI way from one bit of entanglement using projective nondemolition or general demolition measurements is upper bounded by *two*, and Acín *et al.* [7] have proven analytically that this maximum can be *saturated* using a protocol based on a simultaneous maximal quantum violation of *three* Clauser-Horne-Shimony-Holt (CHSH) Bell inequalities [8]. Question (ii) is still open. Intriguingly, Acín *et al.* [7] have also conjectured on the basis of numerical evidence that observing the maximum quantum violation of a single Bell inequality called "the elegant Bell inequality" (EBI) [9] is sufficient for the DI certification of two random bits. The fact that the EBI requires fewer settings than three CHSH Bell inequalities makes this conjecture interesting and worth trying to prove analytically. In this paper, we provide such a proof.

II. THE ELEGANT BELL INEQUALITY

The EBI is a bipartite Bell inequality introduced by Gisin [9] in which one of the parties, Alice, chooses among three dichotomic measurement settings, while the other party, Bob, chooses among four dichotomic measurement settings. If the possible outcomes are ± 1 and $E_{k,l}$ denotes the mean value of the product of the outcomes of Alice's kth and Bob's lth settings, the EBI reads

$$S \equiv E_{1,1} + E_{1,2} - E_{1,3} - E_{1,4} + E_{2,1} - E_{2,2} + E_{2,3} - E_{2,4} + E_{3,1} - E_{3,2} - E_{3,3} + E_{3,4} \leqslant 6. \quad (1)$$

Its maximum quantum violation is $S = 4\sqrt{3}$ [7].

Besides the practical aspect that the EBI requires fewer settings than three CHSH Bell inequalities, there is also the exciting possibility that the answer to question (ii) would be the EBI. This would be remarkable. The adjective "elegant" in the EBI comes from the observation that its maximal quantum violation is achieved when Alice and Bob share an ebit, the eigenstates of Alice's three projective measurements form a complete set of three mutually unbiased bases (MUBs), and the eigenstates of Bob's four projective measurement can be divided into two sets, each of which defines a symmetric informationally complete positive operator-valued measure (SIC-POVM). MUBs and SIC-POVMs are two geometric structures of independent interest [10] and the fact that both might be simultaneously necessary for the optimal DI certification of maximal randomness from maximal entanglement would be quite surprising.

[*]ole.andersson@fysik.su.se
[†]piotr.badziag@gmail.com
[‡]irina.dumitru@fysik.su.se
[§]adan@us.es

Acín *et al.* [7] have proposed a strategy for proving analytically that the EBI can be used for the DI certification of two random bits from one ebit. The strategy relies on the assumption that the maximal violation of the EBI is self-testing. We have recently proven [11] that the maximal violation of the EBI is not self-testing in the sense of Refs. [12,13]. However, the conjecture still holds and we prove it through a different strategy than the one proposed in Ref. [7].

III. SCENARIO

We are interested in the following scenario. Alice has a source of systems and a measurement device with four outcomes. She uses them to perform a four-outcome measurement on each system produced by the source. The generated outcomes are apparently unpredictable, i.e., after many measurements, Alice notices that the four outcomes appear with the same frequency and follow no pattern. However, it might be that the outcomes are not so unpredictable as it seems and someone else might be able to guess the outcomes of Alice's measurements. That someone, whom we call the adversary, or Eve, could also be the manufacturer of Alice's device. This means that the device is untrusted and that Alice is therefore interested in a device-independent certification of the randomness. Here we propose two tests that Alice can perform to make sure that her device generates outputs which are completely unpredictable for everyone. The tests, if passed, certify that the local guessing probability of Eve does not exceed the minimal value 1/4. If and only if this is so, we say that Alice's measurement produces two random bits.

IV. TESTS

If we write A_4 for Alice's four-outcome POVM and model Eve's substantiated guesses as outcomes a of a local four-outcome POVM F (if Eve measures a she guesses that Alice measured a), the *local guessing probability* of Eve is

$$G = \max_F \sum_a P(a,a|A_4,F). \tag{2}$$

The sum equals the probability that Eve makes a correct guess given that Alice measures A_4 and Eve measures F. We maximize over all four-outcome POVMs that are local to Eve. The tests then certify that $G = 1/4$.

The tests involve a third party, Alice's trusted friend Bob, who has access to a second system generated simultaneously by Alice's source. The scenario is sketched out in Fig. 1.

For the tests, Alice needs three and Bob needs four measurement settings measuring local dichotomic observables. We write A_1, A_2, A_3 and B_1, B_2, B_3, B_4 for Alice's and Bob's observables, respectively, and take their outcomes to be -1 and $+1$. We also write $E_{k,l}$ for the expectation value of the products of the outcomes of Alice's kth and Bob's lth measurement and $E_{a|k,l}$ for the expectation value of Bob's lth measurement which is conditioned on the outcome of Alice's

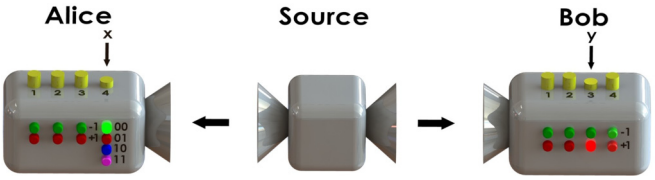


FIG. 1. The source simultaneously emits two systems, one to each side. Buttons represent possible measurements. Light bulbs represent possible outcomes. Alice and Bob wants to certify in a device-independent way that the two bits produced when Alice presses her button 4 are actually random (i.e., unpredictable even for an adversary who manufactured the devices).

kth measurement, i.e.,

$$E_{k,l} = \sum_{a,b} ab\, P(a,b|A_k,B_l), \tag{3a}$$

$$E_{a|k,l} = \sum_b b\, P(a,b|A_k,B_l). \tag{3b}$$

A test for the source. The first test is a Bell test. To pass the test, Alice's and Bob's dichotomic measurements should generate statistics indicating that the EBI is maximally violated: $S = 4\sqrt{3}$.

A test for the measurement device. A necessary requirement for $G = 1/4$ is that Alice's device generates an apparently random output, i.e., $P(a|A_4) = 1/4$ for all outcomes a. We define a family of four qubit operators $Q = \{Q_a\}$ by

$$Q_a = \gamma_a^0 \mathbb{1} + \gamma_a^1 Z + \gamma_a^2 X + \gamma_a^3 Y, \tag{4}$$

where Z, X, Y are the Pauli operators and

$$\gamma_a^0 = P(a|A_4), \tag{5a}$$

$$\gamma_a^1 = \frac{\sqrt{3}}{2}(E_{a|4,1} + E_{a|4,2}), \tag{5b}$$

$$\gamma_a^2 = \frac{\sqrt{3}}{2}(E_{a|4,1} + E_{a|4,3}), \tag{5c}$$

$$\gamma_a^3 = -\frac{\sqrt{3}}{2}(E_{a|4,2} + E_{a|4,3}). \tag{5d}$$

The second test is passed if $P(a|A_4) = 1/4$ and Q is an *extremal* four-outcome qubit POVM. Here Bob uses the same three observables B_1, B_2, B_3 used in the first test. Below we describe how to determine that Q is an extremal POVM.

Since the tests only require an analysis of the measurement statistics and assume nothing about either the devices used to generate this statistics or the measurement device used by Eve, they ensure that the randomness generated by Alice is genuine and device-independent.

The simplest scenario that passes the two tests is the following. Suppose that Alice and Bob share two qubits in the singlet state,

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{6}$$

If Alice measures three dichotomic observables which correspond to the Pauli observables

$$A_1 = Z, \quad A_2 = X, \quad A_3 = Y, \tag{7}$$

and Bob measures four observables which correspond to

$$B_1 = \frac{1}{\sqrt{3}}(Z + X - Y),\ B_3 = \frac{1}{\sqrt{3}}(-Z + X + Y), \quad (8a)$$

$$B_2 = \frac{1}{\sqrt{3}}(Z - X + Y),\ B_4 = \frac{1}{\sqrt{3}}(-Z - X - Y), \quad (8b)$$

then the EBI is maximally violated, which means the first test is passed. Furthermore, if Alice measures the four-outcome POVM A_4 whose elements correspond to the four linearly independent unit rank projectors

$$A_{1|4} = \frac{1}{4}\left[\mathbb{1} - \frac{1}{\sqrt{3}}(Z + X + Y)\right], \quad (9a)$$

$$A_{2|4} = \frac{1}{4}\left[\mathbb{1} - \frac{1}{\sqrt{3}}(Z - X - Y)\right], \quad (9b)$$

$$A_{3|4} = \frac{1}{4}\left[\mathbb{1} + \frac{1}{\sqrt{3}}(Z - X + Y)\right], \quad (9c)$$

$$A_{4|4} = \frac{1}{4}\left[\mathbb{1} + \frac{1}{\sqrt{3}}(Z + X - Y)\right], \quad (9d)$$

then Q defined by Eq. (4) equals A_4, which is extremal according to the discussion in Sec. VI. The requirement $P(a|A_4) = 1/4$ is also satisfied and, hence, the second test is also fulfilled.

V. PROOF

We now prove that for any quantum state $|\psi\rangle$ generated by Alice's source and shared with Bob and Eve, and for any A_1, A_2, A_3, A_4 local to Alice, B_1, B_2, B_3, B_4 local to Bob, and F local to Eve, if the two tests have been passed, then $\sum_a P(a,a|A_4,F) = 1/4$ and therefore $G = 1/4$.

In Ref. [11], we have shown that a maximal violation of the EBI implies the existence of an isometry $\Phi = \Phi_A \otimes \Phi_B \otimes \mathbb{1}_E$,

$$\begin{aligned}\Phi : \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E &\to (\mathcal{H}_A \otimes \mathcal{H}_2) \otimes (\mathcal{H}_B \otimes \mathcal{H}_2) \otimes \mathcal{H}_E \\ &= (\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E) \otimes (\mathcal{H}_2 \otimes \mathcal{H}_2),\end{aligned} \quad (10)$$

such that $\Phi(|\psi\rangle) = |\chi\rangle \otimes |\phi_+\rangle$ for some $|\chi\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ and such that

$$\begin{aligned}\Phi(B_1|\psi\rangle) = \frac{1}{\sqrt{3}}\{&|\chi\rangle \otimes [\mathbb{1} \otimes (Z + X)|\phi_+\rangle] \\ &- J|\chi\rangle \otimes (\mathbb{1} \otimes Y|\phi_+\rangle)\},\end{aligned} \quad (11a)$$

$$\begin{aligned}\Phi(B_2|\psi\rangle) = \frac{1}{\sqrt{3}}\{&|\chi\rangle \otimes [\mathbb{1} \otimes (Z - X)|\phi_+\rangle] \\ &+ J|\chi\rangle \otimes (\mathbb{1} \otimes Y|\phi_+\rangle)\},\end{aligned} \quad (11b)$$

$$\begin{aligned}\Phi(B_3|\psi\rangle) = \frac{1}{\sqrt{3}}\{&|\chi\rangle \otimes [\mathbb{1} \otimes (-Z + X)|\phi_+\rangle] \\ &+ J|\chi\rangle \otimes (\mathbb{1} \otimes Y|\phi_+\rangle)\},\end{aligned} \quad (11c)$$

$$\begin{aligned}\Phi(B_4|\psi\rangle) = \frac{1}{\sqrt{3}}\{&|\chi\rangle \otimes [\mathbb{1} \otimes (-Z - X)|\phi_+\rangle] \\ &- J|\chi\rangle \otimes (\mathbb{1} \otimes Y|\phi_+\rangle)\}.\end{aligned} \quad (11d)$$

Here, $\mathcal{H}_A$, $\mathcal{H}_B$, and $\mathcal{H}_E$ are the Hilbert spaces of Alice, Bob, and Eve, $\mathcal{H}_2$ is a two-dimensional Hilbert space with a computational basis $\{|0\rangle, |1\rangle\}$, the state $|\phi_+\rangle$ is the two-qubit singlet state defined in Eq. (6), and J is an involution (i.e., J^2 is the identity) on the support of $\Phi_B \otimes \mathbb{1}_E$ which commutes with every operator local to Eve.

On the support of Φ_A, each $A_{a|4}$, i.e., the element of A_4 corresponding to outcome a, can be represented by an operator R_a acting on $\mathcal{H}_A \otimes \mathcal{H}_2$. If we expand R_a as

$$R_a = R_a^0 \otimes \mathbb{1} + R_a^1 \otimes Z + R_a^2 \otimes X + R_a^3 \otimes Y, \quad (12)$$

where each R_a^k is a Hermitian operator on $\mathcal{H}_A$, then

$$\gamma_a^0 \equiv \langle\psi|A_{a|4}|\psi\rangle = \langle\chi|R_a^0|\chi\rangle, \quad (13a)$$

$$\gamma_a^1 \equiv \frac{\sqrt{3}}{2}\langle\psi|A_{a|4}(B_1 + B_2)|\psi\rangle = \langle\chi|R_a^1|\chi\rangle, \quad (13b)$$

$$\gamma_a^2 \equiv \frac{\sqrt{3}}{2}\langle\psi|A_{a|4}(B_1 + B_3)|\psi\rangle = \langle\chi|R_a^2|\chi\rangle, \quad (13c)$$

$$\gamma_a^3 \equiv -\frac{\sqrt{3}}{2}\langle\psi|A_{a|4}(B_2 + B_3)|\psi\rangle = \langle\chi|R_a^3 J|\chi\rangle. \quad (13d)$$

The family of operators $Q = \{Q_a\}$ on $\mathcal{H}_2$ defined by

$$Q_a = \gamma_a^0\mathbb{1} + \gamma_a^1 Z + \gamma_a^2 X + \gamma_a^3 Y \quad (14)$$

forms an extremal four-outcome POVM by the second test.

The operator J is diagonalizable with eigenvalues -1 and $+1$. We write $J_\pm$ for the orthogonal projections onto its ± 1 eigenspaces. Also, inspired by Acín *et al.*, we define normalized states $|\varphi_{\pm,a}\rangle$ by

$$|\varphi_{\pm,a}\rangle = J_\pm F_a|\chi\rangle/\sqrt{q_{\pm,a}}. \quad (15)$$

Then,

$$\begin{aligned}\gamma_a^k &= \sum_{a'}\langle\chi|F_{a'}J_+R_a^kJ_+F_{a'}|\chi\rangle + \langle\chi|F_{a'}J_-R_a^kJ_-F_{a'}|\chi\rangle \\ &= \sum_{a'} q_{+,a'}\langle\varphi_{+,a'}|R_a^k|\varphi_{+,a'}\rangle + q_{-,a'}\langle\varphi_{-,a'}|R_a^k|\varphi_{-,a'}\rangle \\ &\equiv \sum_{a'} q_{+,a'}\beta_a^{k;+,a'} + q_{-,a'}\beta_a^{k;-,a'},\end{aligned} \quad (16)$$

for $k = 0,1,2$, and

$$\begin{aligned}\gamma_a^3 &= \sum_{a'}\langle\chi|F_{a'}J_+R_a^3J_+F_{a'}|\chi\rangle - \langle\chi|F_{a'}J_-R_a^3J_-F_{a'}|\chi\rangle \\ &= \sum_{a'} q_{+,a'}\langle\varphi_{+,a'}|R_a^3|\varphi_{+,a'}\rangle - q_{-,a'}\langle\varphi_{-,a'}|R_a^3|\varphi_{-,a'}\rangle \\ &\equiv \sum_{a'} q_{+,a'}\beta_a^{3;+,a'} - q_{-,a'}\beta_a^{3;-,a'}.\end{aligned} \quad (17)$$

Here we have, without loss of generality, assumed that F is projective. Next, define four-outcome qubit POVMs $R^{\pm,a'} = \{R_a^{\pm,a'}\}$ as

$$R_a^{+,a'} = \beta_a^{0;+,a'}\mathbb{1} + \beta_a^{1;+,a'}Z + \beta_a^{2;+,a'}X + \beta_a^{3;+,a'}Y, \quad (18a)$$

$$R_a^{-,a'} = \beta_a^{0;-,a'}\mathbb{1} + \beta_a^{1;-,a'}Z + \beta_a^{2;-,a'}X - \beta_a^{3;-,a'}Y. \quad (18b)$$

From Eqs. (16) and (17) follow that $Q_a = \sum_{\pm,a'} q_{\pm,a'}R_a^{\pm,a'}$, which is a convex decomposition of Q. Since Q is extremal,

$R_a^{\pm,a'} = Q_a$ and, hence, $\beta_a^{k;\pm,a'} = \gamma_a^k$ for all a'. In particular, $\beta_a^{0;\pm,a} = \gamma_a^0 = 1/4$ for all a. Now,

$$\begin{aligned}\sum_a P(a,a|A_4,F) &= \sum_a \langle\psi|A_{a|4}F_a|\psi\rangle \\ &= \sum_a \langle\chi|R_a^0 F_a|\chi\rangle \\ &= \sum_a \langle\chi|F_a J_+ R_a^0 J_+ F_a|\chi\rangle \\ &\quad + \langle\chi|F_a J_- R_a^0 J_- F_a|\chi\rangle \\ &= \sum_a q_{+,a}\beta_a^{0;+,a} + q_{-,a}\beta_a^{0;-,a} \\ &= 1/4. \end{aligned} \tag{19}$$

Since we have not assumed anything about Eve's measurement, this proves that $G = 1/4$.

VI. EXTREMAL QUBIT POVMs

POVMs of a fixed number of outcomes form a convex set. Its extremal elements are those that cannot be written as nontrivial convex combinations of other POVMs. D'Ariano *et al.* [6] have classified all extremal POVMs with discrete output sets. According to this classification, a four-outcome qubit POVM is extremal if, and only if, it consists of four linearly independent one-dimensional projectors. The elements of Q defined by Eq. (4) are one-dimensional projectors provided that $\mathrm{tr}\, Q_a > 0$ and $\det Q_a = 0$. The former condition is satisfied if $P(a|A_4) > 0$ and the latter condition is satisfied if

$$\begin{aligned}(E_{a|4,1} + E_{a|4,2})^2 + (E_{a|4,1} + E_{a|4,3})^2 \\ + (E_{a|4,2} + E_{a|4,3})^2 = \tfrac{4}{3}P(a|A_4)^2,\end{aligned} \tag{20}$$

for all a. Moreover, the projectors are linearly independent provided the vectors $[\gamma_a^0\ \gamma_a^1\ \gamma_a^2\ \gamma_a^3]^T$ are linearly independent, where the γ_a^ks are defined as in Eq. (5). Given that $\gamma_a^0 = P(a|A_4) = 1/4$ for all a, this is equivalent to the condition that the matrix of conditional expectation values,

$$\begin{bmatrix} E_{1|4,1} & E_{1|4,2} & E_{1|4,3} \\ E_{2|4,1} & E_{2|4,2} & E_{2|4,3} \\ E_{3|4,1} & E_{3|4,2} & E_{3|4,3} \end{bmatrix}, \tag{21}$$

has full rank.

VII. CONCLUSIONS

We have proven that as conjectured by Acín *et al.* in Ref. [7], the maximal quantum violation of the elegant Bell inequality can be used to certify, in a device-independent way, two bits of randomness from one ebit. This demonstrates how fundamental tools in quantum information, namely, an ebit, a complete set of qubit MUBs, and the elements of qubit SIC-POVMs, are connected to maximal randomness. An open question is whether a certification similar to ours would be possible with fewer measurement settings. If not, this would sharpen the elegance of the protocol and strengthen the surprising connection between complete sets of MUBs and SIC-POVM elements, on one side, and optimal maximal randomness from maximal entanglement, on the other.

Concerning the practical aspects of randomness generation, it should be mentioned that violating different Bell inequalities is not equally costly in terms of statistics [14,15]. Moreover, to certify device-independent generation of more that one random bit from an ebit, it is often better to use a three-outcome POVM rather than a four-outcome POVM since the former is generally more robust against imperfections in the experimental setup [16].

ACKNOWLEDGMENTS

We thank Ingemar Bengtsson for fruitful discussions and for proposing improvements to the text. We also thank Gustavo Cañas for his help with Fig. 1. A.C. acknowledges support from Project No. FIS2014-60843-P, "Advanced Quantum Information" (MINECO, Spain), with FEDER funds, the FQXi Large Grant "The Observer Observed: A Bayesian Route to the Reconstruction of Quantum Theory," and the project "Photonic Quantum Information" (Knut and Alice Wallenberg Foundation, Sweden).

[1] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2006; arXiv:0911.3814.

[2] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[3] A. Acín and L. Masanes, Certified randomness in quantum physics, Nature (London) **540**, 213 (2016).

[4] J. S. Bell, On the Einstein Podolsky Rosen Paradox, Physics **1**, 195 (1964).

[5] S. Popescu and D. Rohrlich, The joy of entanglement, in *Introduction to Quantum Computation and Information*, edited by H. Lo, S. Popescu, and T. Spiller (World Scientific, New York, 1998), p. 29.

[6] G. M. D'Ariano, P. L. Presti, and P. Perinotti, Classical randomness in quantum measurements, J. Phys. A: Math. Gen. **38**, 5979 (2005).

[7] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A **93**, 040102(R) (2016).

[8] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).

[9] N. Gisin, Bell inequalities: Many questions, a few answers, in *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony*, edited by W. C. Myrvold and J. Christian, The Western Ontario Series in Philosophy of Science Vol. 73 (Springer, Netherlands, 2009), p. 125.

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

[11] O. Andersson, P. Badziąg, I. Bengtsson, I. Dumitru, and A. Cabello, Self-testing properties of Gisin's elegant Bell inequality, Phys. Rev. A **96**, 032119 (2017).

[12] M. McKague and M. Mosca, Generalized self-testing and the security of the 6-state protocol, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by W. van Dam, V. M. Kendon, and S. Severini, Lecture Notes in Computer Science Vol. 6519 (Springer, Berlin, 2010), p. 113.

[13] M. McKague, Quantum information processing with adversarial devices, Ph.D. thesis, University of Waterloo, 2010; arXiv:1006.2352.

[14] A. Peres, Bayesian analysis of Bell inequalities, Fortschr. Phys. **48**, 531 (2000).

[15] R. D. Gill, Statistics, causality and Bell's theorem, Statist. Sci. **29**, 512 (2014).

[16] S. Gómez, A. Mattar, E. S. Gómez, D. Cavalcanti, O. Jiménez Farías, A. Acín, and G. Lima, Experimental nonlocality-based randomness generation with non-projective measurements, arXiv:1711.10294.