Exploring the Elegant Bell Inequality

Irina Dumitru

Akademisk avhandling för avläggande av licentiatexamen vid
Stockholms universitet, Fysikum
December 2017

Contents

Acknowledgments

Thank you Ingemar for being a great supervisor. Special thanks to Ole, for discussions, support, advice, as well as to Mohamed. I would also like to thank my colleagues in KOMKO and KIKO for creating a pleasant work environment, and Pil for proofreading. Thanks also to my co-supervisor Jonas and my mentor Michael.

Abstract

In quantum information, device independent certification is a matter of both practical and fundamental interest. In this thesis, we explore the use of a particular Bell inequality, known as the elegant Bell inequality, in device independent certification. We first characterize all states and measurements that can lead to a maximal violation of the elegant Bell inequality. It turns out that, in all cases, the state involved in a maximal violation is a generalized singlet state, and the measurements of one of the parties are always maximally spread out on the Bloch sphere, forming a complete set of mutually unbiased bases. The measurements involved on the other party form two pairs of symmetric informationally complete vectors. The elegant Bell inequality, then, can be used to certify the presence of these elements.

We also explore the usefulness of the elegant Bell inequality in randomness certification, in particular in a protocol for certification of maximal randomness from one entangled bit.

The last part of this thesis is dedicated to a study of some of the special geometric structures involved in the maximal violation of the elegant Bell inequality, namely the symmetric informationally complete vectors. The problem of the existence and of the construction of these sets of vectors in Hilbert spaces of any dimension is open, but there are solutions available in many dimensions. We look at these structures from both a geometric and an algebraic number theory perspective, and conjecture a relation between vectors in different dimensions. We introduce the relation of "alignment" between such sets of vectors.

List of accompanying papers

Paper I **Self-testing properties of Gisin's elegant Bell inequality**
O. Andersson, P. Badziąg, I. Bengtsson, I. Dumitru, A. Cabello.
Physical Review A 96.3 (2017)

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

Paper II **Certification of two bits of randomness from one entangled bit using the elegant Bell inequality**
O. Andersson, P. Badziąg, I. Dumitru, and A. Cabello.
arXiv preprint arXiv:1707.00564 (2017)

I participated in blackboard discussions.

Paper III **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)

I ran numerical calculations in the early stages of the project, to check conjectures and eliminate false leads.

1 Introduction

Classical information theory started by abstracting away from the physical support of information (be it a piece of paper on which the information is represented by wiggly lines, or transistors in a computer where the information is represented by electrical pulses and indentations in ceramic discs) and produced theorems that apply to all classical physical systems, such as *Shannon's noisy channel coding theorem*, as well as designed protocols which can be implemented on different systems (see [1] for logical gates with soldier crabs). Classical information theory makes, in fact, one assumption about the support of information, namely that it be classical. The deepest consequences of this are that the unit of information, the bit, takes two possible values, 0 or 1, and that interrogating the system for this value does not affect the bit.

Quantum information theory aims at studying quantum systems from an information-theoretical perspective, and thus, makes just as little assumptions about the systems it studies: that they obey the laws of quantum mechanics.

Quantum computation and applied quantum information deal with, among other things, tasks involving security and cryptography [2]. In many applications in these directions, adversarial scenarios are taken into consideration, such as two parties trying to communicate in the presence of an eavesdropper, or one party trying to generate random numbers while an adversary is trying to control or guess the numbers. In these scenarios, we are interested in two kinds of research questions: i) answering general questions such as what is the maximum randomness one can hope for under specific circumstances, or the maximum information an eavesdropper can gather before being detected, and ii) constructing protocols for solving different task, and, in particular, constructing optimal protocols. In adversarial scenarios, we need to assume that we are operating with sources and detectors we do not trust. It becomes then a practical question to try and guarantee, from collecting statistics alone, that the devices do what we want them to. This kind of guarantee is called certification. Things we are interested in certifying include the dimension of the states involved, that is to say that the interesting degree of freedom is not entangled with some others (polarization of photons is separable from the angular momentum; electronic levels of ions from their motional modes)[3], that the randomness in a randomness generation protocol is genuine [2] etc. This can in fact be done in quantum

mechanics, it's called device-independent certification [2]. This kind of research is interested in developing protocols that don't involve any model of the devices. The reason certification works is that in many applications and protocols we use non-local correlations as a resource, and the presence of correlations in a certain amount is both necessary and sufficient to validate that the protocol works. Therefore certification can, in many cases, consist of verifying the presence of these correlations. Most known protocols use Bell inequalities, or equivalently, prepare and measure scenarios, to probe the presence of non-local correlations. Aside from the practical considerations, there are fundamental implications of certification, such as the legitimacy of the treatment of correlations as resources (a key aspect of the quantum computing paradigm), or the possibility of singling out quantum mechanics among non-local theories. Our work focuses on one particular Bell inequality, the so-called *elegant Bell inequality*, whose usefulness I investigate in the context of two different certification protocols.

In the next chapter, we give a brief introduction to Bell inequalities and to correlations, using the Clauser-Horne-Shimony-Holt inequality as an example. We then introduce the elegant Bell inequality.

In the following chapter we introduce the concepts of self testing and randomness certification. We then give an account of the elegant Bell inequality in relation to these concepts. We introduce Mutually Unbiased Bases (MUBs) and Symmetric Informationally Complete POVMs (SICs) as geometric structures in the Hilbert space, singled out by the self-testing properties of the elegant Bell inequality. This chapter should equip the reader to follow the first two accompanying papers.

The final chapter is dedicated to Symmetric Informationally Complete POVMs (SICs). We investigate aspects of these objects from geometric and number-theory approaches, and find a connection between SICs in the Hilbert space of dimension d and those in the Hilbert space of dimension $d(d-2)$. We overview numerical results pertaining to dimensions $d*d$ and $d(d-1)$ as well.

2 Bell inequalities

Bell proved in 1964 that quantum mechanics makes predictions that are incompatible with any theory satisfying local realism[4] (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 function of probabilities that is upper bounded by any theory that assumes local realism. Quantum mechanics allows for larger values of the function, therefore 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 2 outcomes, but we don't loose any intuition by restricting to this simple case. In discussing quantum mechanics in terms of probabilities and correlations, we follow Brunner et al [6].

Let Alice have at her disposal n measurement settings, and Bob have m. In each run of the experiment, each parties 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 defined as:

$$E(A_iB_j) = \sum_{a,b} ab \cdot p(ab|A_iB_j) \tag{1}$$

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 $E(A_iB_j)$ has a value, even if it is not measured. We will, from now on, assume, for the sake of simplicity, that it holds, and it is locality, actually, that is violated by quantum mechanics.

A scenario is completely characterized by a total of $4mn$ such joint probabilities (iterating all possible settings $m*n$, and all four possible outcomes). Using terminology introduced by Tsirelson [5], we call the set

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

of all these probabilities *a behavior*. 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 we are interested in: non-signaling behaviors, quantum behaviors, and local realist behaviors.

Non-signaling correlations

The non-signaling constraint (first formalized in [7]) is that the marginal probabilities of one of the parties be independent of the other's measurement setting:

$$\sum_b p(ab|A_iB_j) = \sum_b p(ab|A_iB_k)$$
$$\sum_a p(ab|A_iB_j) = \sum_a p(ab|A_kB_j). \tag{2}$$

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

We can now form an idea of what locality means. A hidden variables theory usually assumes that there exist some other variables, λ, on which the outcomes a and b depend. This hidden factors 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 would be $p(ab|A_iB_j, \lambda)$. Locality then means that the behavior factorizes:

$$p(ab|A_iB_j, \lambda) = p(a|A_i, \lambda)p(b|B_j\lambda). \tag{3}$$

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:

$$p(ab|A_iB_j) = \int_\lambda f(\lambda)p(a|A_i, \lambda)p(b|B_j\lambda)d\lambda \tag{4}$$

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 Hilbert spaces where Alice's and Bob's part of the shared state belongs ($\mathcal{H}_A$ and $\mathcal{H}_B$, respectively). A quantum behavior, then, is any behavior for which a state and two sets of operators, as defined above, can be found such that:

$$p(ab|A_iB_j) = Tr(\rho_{AB} M_{a|A_i} M_{b|B_j}). \tag{5}$$

This is known in quantum mechanics as *the Born rule*. We can simplify this expression, without loss of generality, by taking the state to be pure and the operators to be projectors, if necessary by increasing the dimension of the Hilbert space. The equation then becomes:

$$p(ab|A_iB_j) = \langle \Psi | M_{a|i} \otimes M_{b|j} | \Psi \rangle. \tag{6}$$

Any quantum behavior satisfies non-signaling constraints, but there exist non-signaling behaviors that are not quantum (for example, the Popescu-Rorlich box, see [7]). Moreover, any local behavior admits a description of the form 5, as shown for example by Pitowsky [8], but there exist quantum behaviors which are not local.

2.0.1 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 [9]. 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 settings i and j respectively:

$$E_{ij} = \langle A_i B_j \rangle = \sum_{a,b} ab \cdot p(ab|A_iB_j). \tag{7}$$

The inequality then reads:

$$S = E_{00} + E_{01} + E_{10} - E_{11} \leq 2, \tag{8}$$

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

The maximum quantum value is

$$S = 2\sqrt{2} > 2 \tag{9}$$

Equation (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 [9].

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 1.). 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.

$\langle A_0 \rangle$	$\langle A_1 \rangle$	$\langle B_0 \rangle$	$\langle B_1 \rangle$	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 1: the local values of S

Incidentally, 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 (5), we obtain a behavior that violates the CHSH inequality. I will give an example of such a choice here (in Section 3.1.1 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 are the Pauli operators acting on Alice's Hilbert space, in the z and x directions, respectively. We choose Bob's operators to be:

$$B_0 = \frac{-Z_B - X_B}{\sqrt{2}} \qquad B_1 = \frac{-Z_B + X_B}{\sqrt{2}}, \tag{10}$$

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 (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

$$F = A_0 B_0 + A_0 B_1 + A_1 B_1 - A_1 B_1. \tag{11}$$

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

$$F^2 = 4\mathrm{I}_{AB} - [A_0, A_1][B_0, B_1]. \tag{12}$$

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

$$\|O\| = \sqrt{\langle O^\dagger O\rangle}, \tag{13}$$

or simply

$$\|O\| = \sqrt{\langle O^2\rangle}, \tag{14}$$

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

$$\|[A_0, A_1]\| \leq 2\|A_0\|\|A_1\| \tag{15}$$

$$\|[B_0, B_1]\| \leq 2\|B_0\|\|B_1\| \tag{16}$$

into equation (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 [7]. 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 (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.

2.0.2 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 $dim\mathcal{L} = dim\mathcal{Q} = dim\mathcal{NS}$ [10]. 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 [11]. They classified the relations between the faces of $\mathcal{L}$, $\mathcal{Q}$, and $\mathcal{NS}$, and concluded that seven distinct cases can occur. Figure 1., 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.

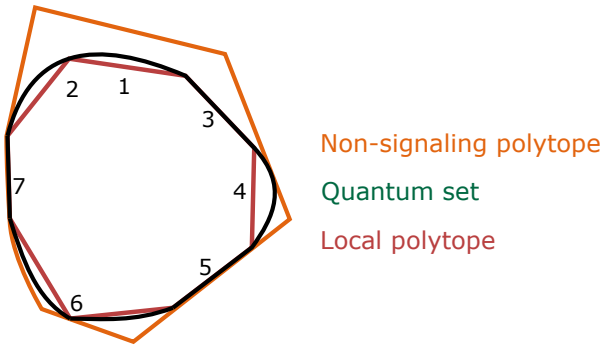

Figure 1: An illustration of a possible slice through the set of probabilities, containing all cases of relations between the faces of the three sets of interest, for a given Bell inequality:

1. Case 1 corresponds to $\beta_L < \beta_Q < \beta_{NS}$
2. Case 2 correspon ds 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 contains a lower dimensional face. 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.

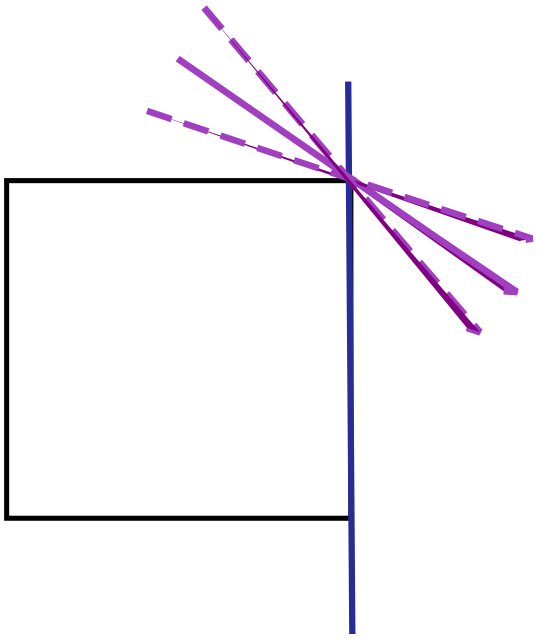

Figure 2: An illustration of hyperplanes containing faces of the local polytope, for the case $d = 2$. The blue line contains a facet (in this case a one dimensional surface, an edge of the square). It uniquely determines a face of the polytope. The solid purple line contains a lower dimensional face (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 [12]. We use a "truth-table" to go over the possible values of S, similar to Table 1., but setting the possible expectation values of each operator are at 0 and 1, so that the formalism resembles Boole 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 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 behaviour 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. The four equivalent CHSH inequalities can be expressed in terms of the vector elements as:

$$-1 \leq v_{E_{00}} + v_{E_{01}} + v_{E_{11}} - v_{E_{10}} - v_{A_0} - v_{B_1} \leq 0 \tag{17a}$$
$$-1 \leq v_{E_{10}} + v_{E_{11}} + v_{E_{01}} - v_{E_{00}} - v_{A_1} - v_{B_1} \leq 0 \tag{17b}$$
$$-1 \leq v_{E_{00}} + v_{E_{01}} + v_{E_{11}} - v_{E_{10}} - v_{A_0} - v_{B_1} \leq 0 \tag{17c}$$
$$-1 \leq v_{E_{00}} + v_{E_{01}} + v_{E_{11}} - v_{E_{10}} - v_{A_0} - v_{B_1} \leq 0 \tag{17d}$$

The number of corners that saturate each of these inequalities is 8, which

means that each of the inequalities defines a facet.

2.0.3 The elegant Bell inequality

The elegant Bell inequality (EBI from here on) is a bipartite Bell inequality introduced by Gisin [13]. 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. We define the Bell operator

$$\begin{aligned}\Sigma =& A_1B_1 + A_1B_2 - A_1B_3 - A_1B_4 + A_2B_1 - A_2B_2 \\ &+ A_2B_3 - A_2B_4 + A_3B_1 - A_3B_2 - A_3B_3 + A_3B_4\end{aligned} \tag{18}$$

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

$$\begin{aligned}S \equiv& E_{1,1} + E_{1,2} - E_{1,3} - E_{1,4} + E_{2,1} - E_{2,2} \\ &+ E_{2,3} - E_{2,4} + E_{3,1} - E_{3,2} - E_{3,3} + E_{3,4} \leq 6\end{aligned} \tag{19}$$

Its maximum quantum value is $S = 4\sqrt{3}$ [23]. The adjective "elegant" in the EBI comes from the observation that its 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 Quantum certification

3.1 Self-testing

The concept of *self-testing* was introduced by Mayers and Yao [14]. 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 [16, 17], 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

$$\langle\,\phi\,|\Pi_\pm^{a_k}\Pi_\pm^{b_l}|\,\phi\,\rangle = \langle\,\psi\,|\Pi_\pm^{A_k}\Pi_\pm^{B_l}|\,\psi\,\rangle \tag{20}$$

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

$$\begin{aligned}\Phi = \Phi_A \otimes \Phi_B : H_A \otimes H_B &\to (H_A \otimes H_a) \otimes (H_B \otimes H_b) \\ &= (H_A \otimes H_B) \otimes (H_a \otimes H_b)\end{aligned} \tag{21}$$

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.

3.1.1 Self-testing property of the CHSH inequality

Popescu and Rohrlich [15] 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 selftesting. 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:

$$\langle\Psi|F|\Psi\rangle = \langle\Psi|A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1|\Psi\rangle = 2\sqrt{2} \tag{22}$$

We use the Schmidt decomposition of a pure qubit state:

$$|\,\Psi\,\rangle = \sum_{i=1}^{n} c_i|\,u_i v_i\,\rangle \tag{23}$$

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 (23). From equation (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:

$$F^2|\,\Psi\,\rangle = 8|\,\Psi\,\rangle \tag{24}$$

Expanding equation 24, and using the fact that $A_i^2 = B_j^2, \forall i, j$ we get

$$\begin{aligned}(4 \;&+\; B_0B_1 + A_0A_1 - A_0A_1B_0B_1 + B_1B_0 + A_0A_1B_1B_0 - A_0A_1 \\ &+\; A_1A_0 + A_1A_0B_0B_1 - B_0B_1 - A_1A_0B_1B_0 - A_1A_0 - B_1A_0)|\,\Psi\,\rangle \\ &=\; 8|\,\Psi\,\rangle,\end{aligned} \tag{25}$$

which we can express as

$$i(A_0A_1 - A_1A_0)i(B_0B_1 - B_1B_0)|\,\Psi\,\rangle = 4|\,\Psi\,\rangle, \tag{26}$$

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

$$\begin{aligned}(i[A_0, A_1])^2|\,\Psi\,\rangle &= -(A_0A_1A_0A_1 - A_0A_1A_1A_0 - A_1A_0A_0A_1 + A_1A_0A_1A_0) \\ &= (2 - (A_0A_1A_0A_1 + A_1A_0A_1A_0))|\,\Psi\,\rangle \\ &= 4|\,\Psi\,\rangle,\end{aligned} \tag{27}$$

which implies

$$(A_0A_1A_0A_1 + A_1A_0A_1A_0)|\,\Psi\,\rangle = -2|\,\Psi\,\rangle, \tag{28}$$

and therefore

$$\langle\Psi|(A_0A_1 + A_1A_0)^2|\Psi\rangle, \tag{29}$$

which means that $|\,\Psi\,\rangle$ is an eigenvector of $A_0A_1 + A_1A_0$ with eigenvalue 0. From the decomposition (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:

$$A_0A_1 + A_1A_0 = 0. \tag{30}$$

Equation (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

$$|\,\Psi\,\rangle = \sum_{ij=1}^{n/2} c_{ij}|\,\alpha_{ij}\,\rangle. \tag{31}$$

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 [14], also concerns the singlet. It was McKague [16, 17] who put these two results in terms of equivalence of experiments. Further developments were produced by Wu et al. [18], 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.

3.1.2 Selt-testing property of the EBI

In our work [19], 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 2.0.3. 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:

$$\langle\Psi|\Sigma|\Psi\rangle = 4\sqrt{3}, \tag{32}$$

where Σ has been defined in Section 2.2. 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 o $|\,\Psi\,\rangle$, 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

$$D_1 = (A_1 + A_2 + A_3)/\sqrt{3}, \tag{33a}$$

$$D_2 = (A_1 - A_2 - A_3)/\sqrt{3}, \tag{33b}$$

$$D_3 = (-A_1 + A_2 - A_3)/\sqrt{3}, \tag{33c}$$

$$D_4 = (-A_1 - A_2 + A_3)/\sqrt{3}. \tag{33d}$$

We can then conclude the following things about the states and operators that satisfy (32):

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

$$H_A^i = \bigoplus_{p=1}^{n_i} H_A^{ip}, \qquad A_k^i = \bigoplus_{p=1}^{n_i} A_k^{ip}. \tag{34}$$

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

$$A_1^{ip} = Z, \qquad A_2^{ip} = X, \qquad A_3^{ip} = \pm Y. \tag{35}$$

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

$$H_B^i = \bigoplus_{p=1}^{n_i} H_B^{ip}, \qquad B_l^i = \bigoplus_{p=1}^{n_i} B_l^{ip}, \tag{36}$$

and the operators admit the decomposition:

$$B_1^{ip} = \tfrac{1}{\sqrt{3}}(A_1^{ip} + A_2^{ip} - A_3^{ip}) = \tfrac{1}{\sqrt{3}}(Z + X \mp Y), \tag{37a}$$

$$B_2^{ip} = \tfrac{1}{\sqrt{3}}(A_1^{ip} - A_2^{ip} + A_3^{ip}) = \tfrac{1}{\sqrt{3}}(Z - X \pm Y), \tag{37b}$$

$$B_3^{ip} = \tfrac{1}{\sqrt{3}}(-A_1^{ip} + A_2^{ip} + A_3^{ip}) = \tfrac{1}{\sqrt{3}}(-Z + X \pm Y), \tag{37c}$$

$$B_4^{ip} = \tfrac{1}{\sqrt{3}}(-A_1^{ip} - A_2^{ip} - A_3^{ip}) = \tfrac{1}{\sqrt{3}}(-Z - X \mp Y). \tag{37d}$$

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

$$\begin{aligned} |\,\psi\,\rangle &= \sum_{i=1}^{m}\sum_{p=1}^{n_i} \lambda_i(|\,0_A^{ip}0_B^{ip}\,\rangle + |\,1_A^{ip}1_B^{ip}\,\rangle) \\ &= \sqrt{2}\sum_{i=1}^{m}\sum_{p=1}^{n_i} \lambda_i|\,\phi_+^{ip}\,\rangle. \end{aligned} \tag{38}$$

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 3.1,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 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 [21]. 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. [20] 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.* [22], who have proven that the maximum number of bits that can be certified in a DI way from one bit of entanglement is upper bounded by *two*. Recently, Acín *et al.* [23] 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 II in this thesis proposes a modified version of this second randomness certification protocol and offers an analytic proof of the certification. Our randomness certification [24] 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 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 testing 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. 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 [24]).

We model Eve's guessing as the application of a local 4-outcome POVM F (if Eve measures a she guesses that Alice measured 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:

$$G = \max_F \sum_a P(a, a|A_4, F). \tag{39}$$

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. We introduce the notation $E_{a|i,j} = \sum_b b\mathrm{p}(ab|A_iB_j)$, 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 (18). That is, they should give rise to $S = 4\sqrt{3}$, where S is defined in (19).

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

$$Q_a = \gamma_a^0 \mathbb{I} + \gamma_a^1 Z + \gamma_a^2 X + \gamma_a^3 Y, \tag{40}$$

where Z, X, Y are the Pauli operators and

$$\gamma_a^0 = P(a|A_4), \tag{41a}$$
$$\gamma_a^1 = \tfrac{\sqrt{3}}{2}(E_{a|4,1} + E_{a|4,2}), \tag{41b}$$
$$\gamma_a^2 = \tfrac{\sqrt{3}}{2}(E_{a|4,1} + E_{a|4,3}), \tag{41c}$$
$$\gamma_a^3 = -\tfrac{\sqrt{3}}{2}(E_{a|4,2} + E_{a|4,3}). \tag{41d}$$

The test is passed if $\mathrm{p}(a|A_4) = 1/4$ and Q is an extremal 4-outcome POVM.

4 Symmetric informationally complete POVMs

We turn our attention now to the geometric objects mentioned earlier (which appeared as descriptions of collection of measurements in scenarios maximally violating the Elegant Bell Inequality), the so-called SIC-POVMs. An alternative, better, name for these structures is SICs [25]. They are structures of independent interest, first introduced in [26, 27]. The question of their existence in all finite dimensions is open, and it is a question of rich structure, that brings together practical considerations in optimal quantum

state characterization and highly abstract considerations in number theory. We first introduce the definition of SIC-POVMs, then give an overview of the properties of all known solutions. We then explore some of the very interesting connections between geometry and algebraic number theory that SICs expose.

4.1 Definition

SIC-POVM stands for symmetric informationally-complete POVM. A POVM 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. (The abbreviation stands for "positive operator-valued measure", and it is being used for historical reasons). SIC-POVMs are POVMs consisting of d^2 elements of dimension d, proportional to projectors, $E_i = \frac{1}{d}M_i$, (where $M_i = |\Psi_i\rangle\langle\Psi_i|$) and obeying:

$$\mathrm{Tr}(M_i M_j) = \frac{1}{d+1} \tag{42}$$

for $\forall i \neq j$.

The name *symmetric informationally complete* encapsulates the importance of these POVMs in quantum state tomography. SICs are informationally-complete in the sense that complete measurement statistics characterize unambiguously any pure or mixed quantum state. This is ensured by having d^2 operators, giving $d^2 - 1$ probabilities (the condition that the set $\{E_i\}$ resolves the identity reduces the number of linearly independent operators by 1), which are enough to characterize a density matrix ρ in dimension d (the matrix is characterized by d^2-1 real parameters, one degree of freedom being reduced by the condition $\mathrm{Tr}\rho = 1$). The symmetry (the fact that they are equiangular) ensures that the information overlap is minimal. A SIC maps each of its d^2 possible measurement outcomes to one of d^2 subnormalised rank-one projectors on the Hilbert space of d-dimensional pure quantum states. SIC-POVMs can be characterized in terms of frame theory [28]. In this context, a set of unit vectors that specifies a SIC-POVM, $\{|\,\Psi_i\,\rangle\}_{i=0}^{d^2-1}$ by $M_i = |\,\Phi_i\,\rangle\langle\,\Phi_i\,|$, is a maximal equiangular tight frame. An equiangular tight frame (ETF) is a set of equal norm vectors in a d-dimensional space with the property that the scalar products of pairs of vectors are identical and minimal. It has been proven [28] that such a set can contain no less than d and no more than d^2 vectors. The minimal ETFs consist of d vectors with

no overlap, they are the orthonormal bases of the space. The maximal ETFs correspond to the objects we are interested in. Geometrically, 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. We will use the term SIC from now on to refer to the set $\{|\,\Phi_i\,\rangle\}$ of d-dimensional vectors, rather than to the set of projectors obtained from them. The problem of the existence of SICs in all finite dimensions is open. Analytical solutions have been found up to dimension 48, complete numerical solutions up to dimension 50 [29, 30]. The highest dimension for which *some* numerical solution has been found is 844 [31]; and up to dimension 151 at least one solution in each dimension has been found.

4.1.1 The Weyl-Heisenberg group

The search for SICs is a search for a set of vectors. It is natural to consider, when searching for a set of vectors, whether the set could be obtained by displacing one of the elements by applying a group of suitable size, i.e. whether the vectors form an orbit under a group. For SICs, it turns out they do, and that the group is the Weyl-Heisenberg group, which has many applications in signal processing and frame theory [32]. In prime dimensions it has been proven, by Zhu [33], that, if a SIC is covariant under any group, it must be covariant under the d-dimensional Weyl-Heisenberg group. In practice, almost all known SICs are covariant under the Weyl-Heisenberg group. The only exception occurs in dimension 8, where a SIC has been found that is an orbit under a different group (this SIC is known as the Hoggar lines).

We do not get involved with the Hoggar lines, and base our study on Weyl-Heisenberg - covariant SICs, i.e. SICs whose elements form an orbit under this group. To be able to define the group, we introduce the unitaries X and Z, acting on the standard basis in dimension d as

$$X|\,k\,\rangle = |\,k+1\,\rangle \tag{43}$$

and

$$Z|\,k\,\rangle = \omega^k|\,k\,\rangle, \tag{44}$$

the addition being modulo d.

We then define the Weyl-Heisenberg displacement operators as

$$D_{i,j} = \tau^{i*j} X^i Z^j. \tag{45}$$

Up to phase factors, there are d^2 displacement operators. They satisfy

$$\mathrm{Tr}(D_{ij}D_{i'j'}) = d\delta_{ii'}\delta_{jj'} \tag{46}$$

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 information, these bases are called nice error bases. The Weyl-Heisenberg group is the group generated by these operators. We introduce the notation $p = \binom{i}{j}$ in order to keep track of indices more easily. It is convenient to characterize a covariant SIC by a fiducial state $|\,\Psi_0\,\rangle$, which is displaced by the Weyl-Heisenberg operators D_{ij} onto the other elements:

$$|\,\Psi_{ij}\,\rangle = D_{ij}|\,\Psi_0\,\rangle \tag{47}$$

where $\tau = e^{\frac{2i\pi}{2}}$. From here on, we will identify a SIC by its fiducial. The choice of fiducials is made from symmetry considerations, which we will get into below.

We define the *overlap phases* in dimension d as

$$e^{i\theta_p} = \sqrt{d+1}\langle\,\Psi_0\,|\,\Psi_p\,\rangle = \sqrt{d+1}\langle\Psi_0|D_p|\Psi_0\rangle \tag{48}$$

for all $i \neq 0$ or $j \neq 0$. Since the Weyl-Heisenberg operators form an orthogonal basis, any operator acting on $\mathcal{C}^d$ admits a unique decomposition

$$A = \sum_p a_p D_{-p}, \quad a_p = \frac{1}{d}\mathrm{Tr}D_p A. \tag{49}$$

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

$$|\Psi_0\rangle\langle\Psi_0| = \frac{1}{d}\sum_p D_{-p}\langle\Psi_0|D_p|\Psi_0\rangle. \tag{50}$$

This tells us immediately that any SIC can be reconstructed from its overlap phases and thus that the set of overlap phases forms an alternative description of a SIC. This will allow us to introduce number theoretical considerations into the study of SICs. The first observation about the overlap phases is that they turn out to be algebraic integers in the algebraic number field that they give rise to. This holds for all known SICs.

The commutation rule for the Weyl-Heisenberg group is

$$D_p D_q = \omega^{<p,q>} D_q D_p, \tag{51}$$

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

$$D_p D_q = \omega^{2^{-1} < p,q >} D_{q+p}. \tag{52}$$

The addition is modulo d. 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 [34]. For this reason, odd and even cases turn out to be very difficult to treat together. We will treat them separately, and focus on the odd case.

4.1.2 Symmetries

The stability group of the fiducial is the set of all matrices U that leave the fiducial unchanged: $|\,\Psi_0\,\rangle = U|\,\Psi_0\,\rangle$. (The notation U does not imply that all the stabilizers will be unitary; some turn out to be anti-unitary). In order to approach the symmetries, let us first introduce the extended Clifford group. The Clifford group is defined as the group of unitary operators that permute the elements of the Weyl-Heisenberg group [34]:

$$U D_p U^\dagger = D_q \tag{53}$$

From now on, we will fix the dimension d to be an odd number. Keeping the earlier convention on labels for the Weyl-Heisenberg elements, the transformation (53) can be written as $U D_p U^\dagger = D_{f(p)}$, where $f(p)$ is a function of p. It can be proven that $f(p)$ is linear in the elements of p: $f(p) = Mp$, with M a 2×2 matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. It is not, however, the case that the Clifford group contains all such 2×2 matrices. The Clifford group acts as:

$$U D_p D_q U^\dagger = U D_p U^\dagger U D_q U^\dagger = D_{Mp} D_{Mq} = \omega^{2^{-1} < Mp, Mq >} D_{Mp+Mq} \tag{54}$$

$$U D_p D_q U^\dagger = \omega^{2^{-1} < p,q >} U D_{p+q} U^\dagger = \omega^{2^{-1} < p,q >} D_{Mp+Mq} \tag{55}$$

From these it follows that we need $< p, q >=< Mp, Mq >$, modulo d. Only the matrices preserving this relation correspond to elements of the Clifford group. The group of 2×2 matrices that generate the Clifford group is SL(2), that is, the set of 2×2 matrices with determinant 1. The Weyl-Heisenberg

unitary can be obtained knowing this transformation rule (the matrix M) through a method proved by Appleby [34].

$$U_M = \frac{e^{i\theta}}{\sqrt{d}} \sum_{s,r=0}^{d-1} \tau^{\beta^{-1}(\delta r^2 - 2rs + \alpha s^2)} |s\rangle\langle r| \tag{56}$$

Zauner [26] conjectured that in every finite dimension, a SIC fiducial can be found that is left invariant by an order 3 unitary. In almost all dimensions, all order 3 unitaries are equivalent, and we usually choose as a representative the matrix:

$$\langle j|U_Z|i\rangle = \frac{e^{i\xi}}{\sqrt{d}} \tau^{ij+j^2}, \tag{57}$$

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

$$dim Z_k = \left\lfloor \frac{d+3-2k}{3} \right\rfloor, \tag{58}$$

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 as well, there exist at least one solution that is stabilized by the class represented by the Zauner unitary, but there exist solutions that are stabilized by some other order-3 unitary.

4.1.3 Number theory aspects

A number theoretical approach to SICs focuses on the matrix elements of the fiducial matrices, and on the overlap phases. While it is not the case in general that the numbers that appear in SICs are easy to write down (one of the fiducial vectors in dimension 48, for example, takes up 50000 A4 pages), the numbers turn out to have other properties that make them simple, in a sense. For all known SIC fiducials, the matrix elements can be expressed in radicals. This has implications for the associated Galois group. Indeed, the numbers that appear in SICs turn out to have very interesting properties from an algebraic number theory point of view [35]. From this point of view, numbers appearing in different SICs also exhibit remarkable connections, a fact which was first discovered by [35].

4.2 Connections between dimensions

Our work on SICs started from the observation that in dimensions 8 and 48 there exist smaller equiangular tight frames embedded in (some of) the SICs. The fiducials showing this property were the ones that had additional symmetries, other than the order-3 Zauner unitary. Both 8 and 48 are of the form $d(d-2)$, with $d = 4$ and $d = 8$, respectively, and the two embedded ETFs consist of the vectors $D_{di,dj}|\,\Phi_0\,\rangle$ and $D_{(d-2)i,(d-2)j}|\,\Phi_0\,\rangle$ in both cases. Equivalently, the operators

$$\Pi_1 = \sum_{i,j=0}^{d-1} |\,\Psi_{(d-2)i,(d-2)j}\,\rangle\langle\,\Psi_{(d-2)i,(d-2)j}\,| \tag{59}$$

and

$$\Pi_2 = \sum_{i,j=0}^{d-3} |\,\Psi_{di,dj}\,\rangle\langle\,\Psi_{di,dj}\,| \tag{60}$$

are projectors with ranks $\frac{d+1}{2}$ and $\frac{(d-2)(d-1)}{2}$ respectively.

We have explicitly checked this property for all dimensions of form $d(d-2)$ for which SICs were, or became, available. Explicitly, they are: 8, 15, 24, 35, 48, 63, 80, 99, 120, 143, 168, 195 and 323.

It seemed that there exists a connection between the complex Hilbert space of dimension N and the smaller subspace onto which the operators Π_1 and Π_2 project, and that the source of this connection might be the *composite* nature of dimension N. Since establishing connections between structures in different dimensions is a promising direction of research in SIC, opening up the possibility of predicting the symmetry subspace where fiducials may lie, thus narrowing the space where we should search for them, we were motivated to investigate other *composite* dimensions.

In the early stages of the project we checked whether similar ETFs would appear in SICs in dimensions of the form $N' = d(d-1)$ and $N'' = d * d$. We checked the operators

$$\Pi_1' = \sum_{i,j=0}^{d-1} |\,\Psi_{(d-1)i,(d-1)j}\,\rangle\langle\,\Psi_{(d-1)i,(d-1)j}\,| \tag{61}$$

and

$$\Pi_2' = \sum_{i,j=0}^{d-2} |\,\Psi_{di,dj}\,\rangle\langle\,\Psi_{di,dj}\,| \tag{62}$$

for N' and the operator

$$\Pi_1'' = \sum_{i,j=0}^{d-1} | \Psi_{di,dj} \rangle\langle \Psi_{di,dj} | \tag{63}$$

for N'', and they turned out to not be projectors. Tabels 3. and 4. contain detailed information on the dimensions of the above operators, as well as the multiplicity of their eigenvalues.

	rank Π_1'	rank Π_2'	mult. Π_1'	mult. Π_2'
12a	9	8	3,3,3	8 distinct eigenvalues
12b	8	6	4,4	3,3
20a	16	20	4,4,4,4	5,5,5,5
20b	16	20	4,4,4,4	5,5,5,5

Table 3: the ranks and multiplicity of eigenvalues, for operators (61) and (62), for dimensions $N' = d(d-1)$

	rank Π_1''	mult. Π_1''
9a	8	1,3,3,1
9b	8	1,1,3,3
16a	8	1,3,3,1
16b	8	1,1,3,3
25a	25	1,3,3,3,3,3,3,3,3
25b	25	3,3,3,3,3,1,3,3,3

Table 4: the ranks and multiplicity of eigenvalues, for operators (63), for dimensions $N'' = d * d$

This result means that there are no ETFs similar to those in dimensions of form N. This geometric feature thus singles out dimensions $d(d-2)$, and our study focuses on them. Our main result, in fact, is that this geometric property is connected to the number-theoretical properties of SICs in these dimensions.

In dimension 8, it happens that any vector belonging to the same Zauner subspace as the highly symmetric SIC 8*b* produces projectors of the same rank

as Π_1 and Π_2, respectively, when displaced by the same Weyl-Heisenberg operators. It is not the case that for higher dimensions the symmetry subspace is enough to guarantee a vector can be displaced into an ETF in this way. We sampled the subspaces in which highly symmetrical fiducials lie and found that the symmetries alone do not account for this geometric property.

Another remarkable property of the projector operator Π_2 is that it consists of very simple numbers $(0, 1, 1/2)$ in the basis in which the fiducial is expressed. For example, this is how the projector operator looks like for fiducial $15d$:

$$\Pi_2 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \\
0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2}
\end{pmatrix}$$

The projectors commute in all cases, and their product projects to a $\left(\frac{d-1}{2}\right)^2$ -dimensional subspace. In the case of N even, this subspace contains 4 SIC vectors $(|\,\Psi_{0,0}\,\rangle, |\,\Psi_{0,2d}\,\rangle, |\,\Psi_{2d,0}\,\rangle, |\,\Psi_{2d,2d}\,\rangle)$, in the case of N odd, only the fiducial is to be found in this subspace.

The number theory connection between SICs in dimension $N = d(d-2)$ and SICs in dimension d manifests in the overlap phases, a fact which was first observed by Gary McConnell and was studied systematically by us. The relevant observation is that overlap phases belong to the abelian extension $\mathcal{Q}(\sqrt{D_N})$, where D is the square-free part of $(N-3)(N+1)$. We see that

for $N = d(d-2)$, $D_N = D_d$:

$$D_N = [d(d-2)-3][d(d-2)+1] = (d^2-2d-3)(d^2-2d+1) = D_d, \quad (64)$$

after eliminating squares. Another, more subtle, observation is that the squares of the overlap phases in dimension d appear as overlap phases in dimension N as well, at certain positions. Namely, all overlap phases $\langle\Psi_0|D_{di,dj}|\Psi_0\rangle$ and $\langle\Psi_0|D_{(d-2)i,(d-2)j}|\Psi_0\rangle$ in dimension N are squares of phases, or inverse of squares of phases, from dimension d. We introduced the notion of *alignment* to describe the relationship between these 2 fiducials [37]. Given how large the number field from which these numbers are drawn is, this is a remarkable property, pointing again towards the possibility of constructing high dimensional SICs from lower dimensional ones.

We conjecture that for each fiducial in dimension d there exist one fiducial in dimension N for which the phases have this property. This property was tested for all the fiducials in dimensions up to 15. In dimension $195 = 15 * (15-2)$ there was only one highly symmetric fiducial available (with order 6 symmetry), aligned with one of the 15-dimensional fiducials. When we reported our conjecture to Andrew Scott, he was able to find three more highly symmetrical fiducials in 195 (two of order 6 and one of order 12), each of them aligned with one of the fiducials in dimension 15 [30] (with this, everything up to and including dimension 15 is checked). Similarly, our observation helped Grassl and Scott find an exact solution in dimension 323 [31].

References

[1] Y. P. Gunji, Y. Nishiyama, A. Adamatzky, (2011). Robust soldier crab ball gate. AIP Conference Proceedings (Vol. 1389, No. 1, pp. 995-998). AIP.

[2] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D.N. Matsukevich, P. Maunz, C. Monroe. Random numbers certified by Bell's theorem. arXiv preprint arXiv:0911.3427. (2009)

[3] J. Ahrens, P. Badziąg, A. Cabello, M. Bourennane. Experimental device-independent tests of classical and quantum dimensions. arXiv preprint arXiv:1111.1277, (2011).

[4] Bell, John S. Einstein–Podolsky–Rosen Experiments in Quantum Mechanics, High Energy Physics And Accelerators: Selected Papers Of John S Bell (With Commentary). 1995. 768-777.

[5] B. Tsirelson. (1993). Quantum Bell-type inequalities. Hadronic Journal Supplement, 8, 329-345.

[6] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, (2014). Bell nonlocality. Reviews of Modern Physics, 86(2), 419.

[7] Popescu, S., Rohrlich, D. (1994). Quantum nonlocality as an axiom. Foundations of Physics, 24(3), 379-385.

[8] Pitowsky, Itamar. The range of quantum probability. Journal of Mathematical Physics 27.6 (1986): 1556-1565.

[9] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed Experiment to Test Local Hidden Variable Theories. Physical Review Letters 24.10 (1970): 549.

[10] S. Pironio. Lifting Bell inequalities. Journal of mathematical physics 46.6 (2005): 062112.

[11] Goh, Koon Tong, et al. "Geometry of the quantum set of correlations." arXiv preprint arXiv:1710.05892 (2017)

[12] I. Pitowsky. From George Boole to John Bell-The Origins of Bell's Inequality, in: Kafatos M. (eds) Bell's Theorem, Quantum Theory and Conceptions of the Universe. Fundamental Theories of Physics, vol 37. Springer, Dordrecht

[13] 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 **73**, edited by W. C. Myrvold and J. Christian (Springer, Netherlands, 2009), p. 125.

[14] 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).

[15] S. Popescu, D. Rohrlich. Which states violate Bell's inequality maximally?, Phys. Lett. A **169**, 411 (1992). Phys. Rev. Lett. **23**, 880 (1969).

[16] 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.

[17] M. McKague, *Quantum Information Processing with Adversarial Devices*, Ph.D. Thesis, University of Waterloo, 2010. arXiv:1006.2352.

[18] Wang, Yukun, Xingyao Wu, and Valerio Scarani. "All the self-testings of the singlet for two binary measurements." New Journal of Physics 18.2 (2016): 025021.

[19] Andersson, O., Badziąg, P., Bengtsson, I., Dumitru, I., Cabello, A.. Self-testing properties of Gisin's elegant Bell inequality. Physical Review A, 2017. 96(3), 032119

[20] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, H. Zbinden (2000) Optical quantum random number generator, Journal of Modern Optics, 47:4, 595-598,

[21] A. Ekert, R. Renner. The ultimate physical limits of privacy. Nature 507.7493: 443-447, (2014)

[22] G. M. D'Ariano, P. L. Presti, and P. Perinotti, Classical randomness in quantum measurements, https://doi.org/10.1088/0305-4470/38/26/010 J. Phys. A: Math. Gen. **38**, 5979 (2005).

[23] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A **93**, 040102(R) (2016).

[24] Andersson, O., Badziąg, P., Bengtsson, I., Dumitru, I., Cabello, A. (2017). Self-testing properties of Gisin's elegant Bell inequality. Physical Review A, 96(3), 032119.

[25] Fuchs, Christopher A., and Rüdiger Schack. "Quantum-bayesian coherence." Reviews of modern physics 85.4 (2013): 1693.

[26] Zauner G., *Quantendesigns. Grundzüge einer nichtkommutativen designtheorie*. PhD thesis, University of Vienna, 1999. Published in English translation: G. Zauner, *Quantum designs: foundations of a noncommutative design theory* Int. J. Quantum Inf. 9 (2011) 445:508

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

[28] Benedetto, John J., and Matthew Fickus. "Finite normalized tight frames." Advances in Computational Mathematics 18.2 (2003): 357-385.

[29] Scott, A. J., and M. Grassl. "Symmetric informationally complete positive-operator-valued measures: A new computer study." Journal of Mathematical Physics 51.4 (2010): 042203.

[30] Scott, A. J. "SICs: Extending the list of solutions." arXiv preprint arXiv:1703.03993 (2017).

[31] Markus Grassl, and Andrew J. Scott. "Fibonacci-Lucas SIC-POVMs." arXiv preprint arXiv:1707.02944 (2017).

[32] Howard S. D., Calderbank A. R., Moran W. "The finite Heisenberg-Weyl groups in radar and communications." EURASIP Journal on Advances in Signal Processing 2006.1 (2006): 085685.

[33] Zhu, Huangjun. "SIC POVMs and Clifford groups in prime dimensions." Journal of Physics A: Mathematical and Theoretical 43.30 (2010): 305305.

[34] Appleby, D. Marcus. "Symmetric informationally complete–positive operator valued measures and the extended Clifford group." Journal of Mathematical Physics 46.5 (2005): 052107.

[35] M. Appleby, S. Flammia, G. McConnell, J. Yard. "SICs and algebraic number theory." Foundations of Physics (2017): 1-18.

[36] Y. I. Manin, Real multiplication and noncommutative geometry (ein Alterstraum), in O. A. Laudal and R. Piene (eds.): The Legacy of Niels Henrik Abel, Springer 2004.

[37] Appleby, M., Bengtsson, I., Dumitru, I., Flammia, S. (2017). Dimension towers of SICs. I. Aligned SICs and embedded tight frames. Journal of Mathematical Physics, 58(11), 112201.