Configurations in Quantum Information

Kate Blanchfield

Department of Physics
Stockholm University

Licentiate thesis

Thesis for the degree of Licentiate in Physics
Department of Physics
Stockholm University
Sweden

Abstract

Measurements play a central role in quantum information. This thesis looks at two types: contextual measurements and symmetric measurements. Contextuality originates from the Kochen-Specker theorem about hidden variable models and has recently undergone a subtle shift in its manifestation. Symmetric measurements are characterised by the regular polytopes they form in Bloch space (the vector space containing all density matrices) and are the subject of several investigations into their existence in all dimensions.

We often describe measurements by the vectors in Hilbert space onto which our operators project. In this sense, both contextual and symmetric measurements are connected to special sets of vectors. These vectors are often special for another reason: they form configurations in a given incidence geometry.

In this thesis, we aim to show various connections between configurations and measurements in quantum information. The configurations discussed here would have been well-known to 19th and 20th century geometers and we show they are relevant for advances in quantum theory today. Specifically, the Hesse and Reye configurations provide proofs of measurement contextuality, both in its original form and its newer guise. The Hesse configuration also ties together different types of symmetric measurements in dimension 3—called SICs and MUBs—while giving insights into the group theoretical properties of higher dimensional symmetric measurements.

Acknowledgements

Thank you to Ingemar for being an excellent supervisor. Thanks also go to my co-supervisor Hoshang and colleagues from Perimeter Institute, Linköping University and the University of Seville. Finally, thank you to my friends at AlbaNova who make this an enjoyable place to work.

Contents

List of accompanying papers

Paper I **A Kochen-Specker inequality from a SIC**
I. Bengtsson, K. Blanchfield and A. Cabello
Phys. Lett. A **376** 374 (2012)

I calculated the two inequalities and helped write the paper.

Paper II **Proposed experiments of qutrit state-independent contextuality and two-qutrit contextuality-based nonlocality**
A. Cabello, E. Amselem, K. Blanchfield, M. Bourennane, I. Bengtsson
Phys. Rev. A **85** 032108 (2012)

I worked on the theoretical parts of the paper, improving the two inequalities and helping to write the paper.

Paper III **Mutually unbiased bases, Heisenberg-Weyl orbits and the distance between them**
K. Blanchfield
contribution to the Växjö conference "Advances in Quantum Theory" (2012)

Chapter 1

Introduction

Quantum mechanics is inherently probabilistic. The outcomes of measurements upon quantum states cannot be predicted with certainty and we are left with a collection of probabilities for various events. While this feature leads to many famous applications in quantum mechanics, such as schemes for detecting faulty bombs[1] or helping prisoners cooperate[2], it also creates a few difficulties in the theory's interpretation and implementation.

The first, and probably most famous, difficulty is the Einstein, Podolsky and Rosen (EPR) paradox [3]. A measurement on one of a pair of sufficiently spatially-separated entangled particles allows an observer to predict the outcome of a measurement on the other particle through the instantaneous collapse of their shared wavefunction. Consequently, the description of quantum mechanics was called incomplete and hidden variables (or, originally, "elements of reality") were ascribed to quantum states at their conception. This ontic interpretation of the wavefunction allows a complete specification of the state using predetermined measurement outcomes, although Bell's theorem [4] shows that the price for this realism is non-locality. Another, less well-known theory concerning hidden variables is the Kochen-Specker theorem [5]. This looks at non-contextual hidden variable models and shows they are inconsistent with the predictions of quantum mechanics.

The second difficulty arising from the probabilistic nature of quantum mechanics is the measurement problem. The outcomes of measurements, whether preassigned by hidden variables or not, are always classical. The quantum state evolves deterministically, following the Schrödinger equation, and yet we cannot predict with certainty the outcome of a measurement

[1] The famous Elitzur–Vaidman bomb testing problem; see [1] for more details.
[2] A quantum version of the prisoner's dilemma game, introduced in [2].

on the state. We are led to the conclusion that at some point during the measurement process—known as the Heisenberg cut—the quantum state becomes classical. This restriction means we cannot determine an unknown quantum state from a single measurement and quantum state tomography becomes a delicate choice of measurements. The best choice turns out to be a symmetric measurement, where best here means the fewest number of measurements and the minimum uncertainty in their statistics.

These symmetric measurements come in two varieties: mutually unbiased bases (MUBs) and symmetric informationally-complete positive operator measures (SICs). In dimension N, SICs are collections of N^2 projectors, usually orbits under a finite group, and have an equal pairwise overlap between every two projectors. They are also studied under the name equiangular lines, which highlights their symmetric structure. MUBs are collections of $N(N+1)$ projectors with an equal overlap among the different bases. Of the two, SICs are considerably harder to construct theoretically as well as being harder to implement experimentally, and while we might expect SICs not to exist in all dimensions, numerical evidence so far suggests that they can always be found (often using a rather heavy duty computer search). Constructing MUBs, on the other hand, follows a fairly straightforward prescription, but only in certain dimensions.

Both contextual and symmetric measurements are important in quantum information theory. Hidden variable models form a large area in the foundations of quantum mechanics and, of these, contextual measurements in particular are gaining interest both theoretically [6–8] and experimentally [2, 9–11]. There have been several discussions and suggestions for the defining feature of quantum mechanics—what property sets it apart from classical physics. The usual answer is often entanglement or non-locality (closely followed by a discussion of the definition of non-locality), but some argue that contextuality is both wider and more fundamental than either of these properties. In particular, contextuality does not need bipartite or multipartite Hilbert spaces and is already in play for the case of qutrits. Paper I and Paper II in this thesis contribute to the area of contextual measurements by providing a new proof of contextuality and testable inequalities. Symmetric measurements are used in quantum cryptography, but a considerable amount of research is aimed towards proving their existence in all dimensions. It is not clear (yet) why SICs can always be found but MUBs in arbitrary dimensions cannot, though any answer in this direction may have interesting implications for the dimensionality of Hilbert space. SICs are also used in foundational aspects of quantum mechanics and play a central role in the quantum Bayesian formulation of quantum mechanics [12]. Paper

III relates to symmetric measurements by examining sets of MUBs in prime dimensions.

So we have mentioned what we will look at in this thesis, but not how. In some sense, the natural vantage point from which to look at quantum information theory is complex projective space. We are in good company; Dirac relied on projective geometry during his work on quantum mechanics [13] and Hilbert co-authored a popular book on the subject [14]. We shall focus on projective configurations, and examine where they emerge and how they can be useful for contextual and symmetric measurements in quantum information.

The thesis is basically divided into two sections, one for each of the two classes of measurements. We begin with contextual measurements and move onto symmetric ones because we believe this to be the order of complexity, but we could have easily organised things the other way around. In Chapter 2 we introduce contextuality and its impact on hidden variable theories, looking in particular at an established theorem of Kochen and Specker and a newer one by Cabello. We shall follow the shift from Kochen and Specker's original logical statement to one concerning inequalities, before discussing a very recent development in contextuality proofs from earlier this year. Configurations are introduced roughly in the middle of the two sections, although they will appear from the beginning and continue to influence things right up until the very end. Chapter 3 covers the two types of symmetric measurement—SICs and MUBs—and we shall briefly go over their existence and construction. An investigation into the structure of SICs and their relation to configurations in low dimensions is also given here. Chapter 4 holds some concluding remarks.

Chapter 2

Contextual measurements

The Kochen-Specker (KS) theorem was first stated in 1967 as a restriction on hidden variable models [5]. It rules out the possibility of describing nature with a non-contextual hidden variable theory by finding a set of Hermitian observables whose outcomes cannot be embedded into the classical set $\{0, 1\}$ in a non-contextual way. The KS theorem was first proved using 117 observables for which every possible mapping from the operators to their eigenvalues arrives at a logical contradiction. We shall briefly go through the argument here.

The Kochen-Specker theorem. *In a Hilbert space with dimension $N > 2$, truth values cannot be non-contextually assigned to a set of observables in a way consistent with quantum mechanics.*

Consider an operator A in a 3-dimensional Hilbert space. Let it have three distinct eigenvalues a_1, a_2 and a_3 with corresponding eigenvectors $|a_1\rangle$, $|a_2\rangle$ and $|a_3\rangle$. We can arrange these vectors in an orthogonality graph, where each vertex on the graph represents a vector and each line joins two orthogonal vectors. Not every graph is an orthogonality graph; it must be realisable in a given dimension, i.e. we must be able to find vectors for every vertex that obey the orthogonality conditions imposed by the graph. An example of a graph with and without an orthogonal representation in $\mathbb{C}^3$ is shown in Figure (2.1), using the vectors given above.

We can form projection measurements onto our vectors via $P_i = |a_i\rangle\langle a_i|$. Projection measurements are essentially "true or false" questions; they tell us whether a state has eigenvalue a_i for measurement A or not. We can label their outcomes, therefore, with the values 1 (true) or 0 (false). Often, this assignment of 1s and 0s is accompanied by colouring the vectors: black if the outcome of the projector is 1 and white if it is 0.

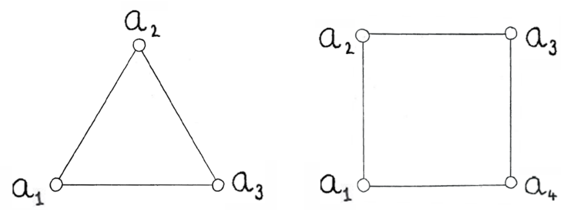

Figure 2.1: Possible graphs in $\mathbb{C}^3$ for the three orthogonal vectors, $|a_1\rangle$, $|a_2\rangle$ and $|a_3\rangle$. The left-hand graph can be realised in 3 dimensions and so constitutes an orthogonality graph. The right-hand graph does not admit a representation in 3 dimensions (although it does in $\mathbb{C}^4$) and so is not an orthogonality graph in $\mathbb{C}^3$.

Orthogonal vectors correspond to compatible projection operators. We make a convenient theoretical assumption that commuting observables can be measured simultaneously as they have a joint eigenbasis. Thus we can imagine the three projectors from Figure (2.1) measured simultaneously in any combination and, according to hidden variable theories, all possessing a pre-existing hidden variable. The hidden variables are assumed to obey the following constraints, called the sum and product rule, respectively:

$$\begin{aligned} P_1 + P_2 = P_3 &\Rightarrow v(P_1) + v(P_2) = v(P_3) \\ P_1 \cdot P_2 = P_3 &\Rightarrow v(P_1) \cdot v(P_2) = v(P_3) \end{aligned} \tag{2.1}$$

where P_1, P_2 and P_3 are mutually compatible and $v(P_1)$, $v(P_2)$ and $v(P_3)$ are their corresponding hidden variables.

If we ask what values our three hidden variables in the orthogonality graph in Figure (2.1) can take, we find that they are subject to some constraints. The projectors are mutually exclusive and so measuring any two projectors together can only result in one instance of the outcome 1. Additionally, as the projectors sum to the identity, their eigenvalues must also sum to 1 (from Equation (2.1)). Returning to the orthogonality graph, we express these constraints as KS colouring rules:

- Two vectors on a line may not both be coloured black.
- Exactly one vector in a complete basis must be coloured black.

The three possible colourings, or mappings, of our orthogonality graph are shown in Figure (2.2).

The assumption of non-contextuality appears when we assign the hidden variables to each vector or projection measurement. The requirement is that the value of a hidden variable does not depend on what other compatible

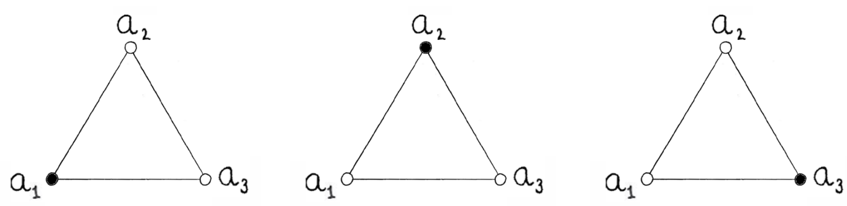

Figure 2.2: Possible colourings for the orthogonality graph in Figure (2.1).

measurements are being simultaneously made. In other words, the hidden variable assigned to the vector a_3 in Figure (2.3) is the same whether we measure P_3 together with P_1 or P_4. Note that $[P_1, P_4] \neq 0$ since they are not connected by a line, so they are incompatible. The collection of projectors measured at the same time is called the context. It is interesting to think about the motivation for non-contextuality. In a way, it is similar to realism, in that it also demonstrates a causal independence between the world and our own actions within it.

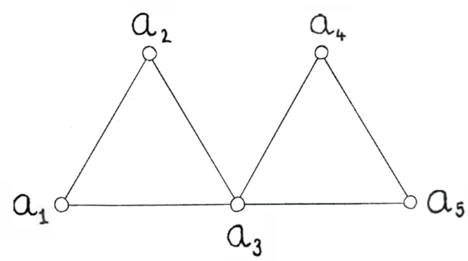

Figure 2.3: A non-contextual assignment of hidden variables requires the value at a_3 be independent of the measurement context, i.e. it does not change when we measure P_3 with P_1 or P_4.

The KS theorem was originally proved using 117 projectors made up from various bases until one projector was forced to take both the colour white and black. From this contradiction, it is clear that non-contextual hidden variables cannot be assigned to this set. In this way, any set of vectors that is uncolourable provides a proof of the KS theorem. We will call such a set interchangeably a KS set or KS proof and give an example of a KS set using 33 vectors in a later section.

There has been interest in trying to reduce the number of vectors required for a KS set [16–20]. The current record for an uncolourable set stands at 31 vectors in 3 dimensions [19] and 18 in 4 dimensions [20]. There have also been several computer searches, including an exhaustive search of up to 30 vectors in $\mathbb{R}^3$ and up to 24 vectors in $\mathbb{R}^4$ [21]. The question of the smallest set with complex vectors is unanswered. We shall look at a few examples of KS sets in the coming sections.

2.1 Correlations

There are obvious parallels between the KS and Bell theorems. Both test, and subsequently constrain, a type of hidden variable theory and it has been shown that it is possible to transform a KS proof in $\mathcal{H}^N$ into a Bell one in $\mathcal{H}^N \otimes \mathcal{H}^N$ when $N > 2$ [8, 22, 23]. It is not so very surprising, then, that the next step for the KS theorem was to translate it into an inequality. We divide the resulting inequalities into two categories: KS inequalities and correlation inequalities, and outline the main points of each here.

A simple and illustrative example of building both types of inequality comes from a set of only 5 measurements in 3 dimensions. The orthogonality graph of the 5 projectors is colourable and so this set isn't usually classed as a KS proof, although, as we shall see later, colourability does not necessarily mean that the set isn't useful for contextuality reasons. We first discuss a KS inequality, starting with the classical version of these 5 measurements and then going on to show how a quantum mechanical treatment noticeably differs.

Assigning variables to the pentagon was first studied by Wright [26], and we shall consider an experiment based on this arrangement. Let each vertex on the pentagon label a possible "yes or no" measurement, say opening a box that may or may not contain a coin, as shown in Figure (2.4).

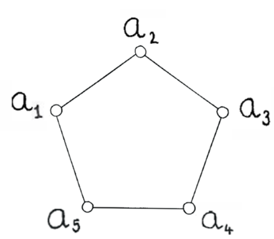

Figure 2.4: The pentagon orthogonality graph. In our experiment, each vertex corresponds to a box that could contain a coin and the five possible measurements of two adjacent boxes are shown by the straight lines. The only possible number of coins, in keeping with the rules, is 2, 1 or 0.

We are allowed to open any two adjacent boxes in one "run" of the experiment, i.e. any boxes connected by a line in Figure (2.4). The coins and boxes have been prepared in advance following one rule: opening two boxes will never reveal two coins. Our model is a non-contextual hidden variable one because we assume the contents of each box (i.e. coin or no coin) is pre-determined and does not change when we open different boxes. We can, like in the KS theorem, assign truth values to the vertices (corresponding to boxes) on the graph in Figure (2.4): a 1 for finding a coin and a 0 for not finding a coin. Now we can perform our experiment to look for the possible assignments of coins. It is clear that the only possibilities for the distribution of the coins are (i) two coins inside non-adjacent boxes, (ii) one coin inside one box, or (iii) no coins in any box. Here, we have employed a statistical assumption—analogous to the fair sampling assumption in Bell's theorem—about the independence of the outcomes from the preparation; specifically, the experiment never possessed an assignment of coins that broke the rule for adjacent boxes in a way that we never saw it.

After repeating the experiment many times, with different preparations of coins and boxes, we can calculate the sum of the average number of coins. We end up with an upper bound for the KS inequality

$$\Sigma_c = \sum_{i=0}^{4} \langle T_i \rangle \leq 2, \tag{2.2}$$

where T_i are the truth values (i.e. the number of coins) from each measurement.

What about the quantum mechanical case? First we need to find 5 vectors that obey the orthogonality conditions

$$\langle a_i | a_{i+2} \rangle = 0 \quad i \in 1, 2, 3, 4, 5, \tag{2.3}$$

with arithmetic modulo 5 understood. Following Klyachko and co-workers, we obtain these vectors from the pentagram in Figure (2.5). Initially the pentagram is lying flat on a plane and each vector begins at the origin in the centre of the pentagram and ends at one of the five vertices. To obtain vectors with the correct orthogonality relations, we raise the vertices up from the plane by shrinking the opening angle of the cone θ (see right-hand side image). To reflect this, we can draw the pentagram orthogonality graph shown on the left-hand side of Figure (2.5). It is just a re-labelling of Figure (2.4) and represents the same orthogonality graph containing 5 vertices and 5 lines.

Explicitly, we use the following five vectors after normalisation

$$(1, 0, x)^\intercal \quad (c, s, x)^\intercal \quad (c\prime, -s\prime, x)^\intercal \quad (c\prime, s\prime, x)^\intercal \quad (c, -s, x)^\intercal$$

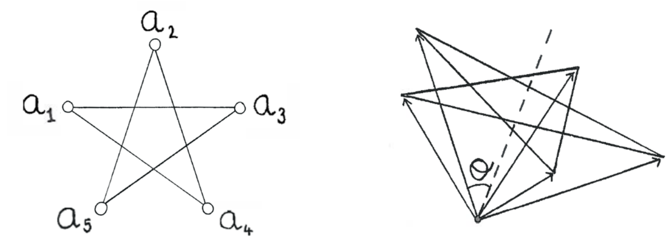

Figure 2.5: The pentagram orthogonality graph (left hand-side) and obtaining the vectors with the correct orthogonalities (right hand-side).

where $x = \sqrt{\cos(\frac{\pi}{5})}$, $c = \cos(\frac{4\pi}{5})$, $s = \sin(\frac{4\pi}{5})$, $c\prime = \cos(\frac{2\pi}{5})$ and $s\prime = \sin(\frac{4\pi}{5})$. Our measurements in the quantum mechanical case correspond to acting with projectors onto these vectors and the KS inequality becomes

$$\Sigma_q = \sum_{i=0}^{4} \mathrm{tr}\left(\rho P_i\right), \tag{2.4}$$

for some state ρ. In order to obtain a discrepancy between the classical result and the quantum mechanical one, we want to maximise Σ_q. This is achieved by taking the largest eigenvalue of the operator $\Sigma = \sum_{i=0}^{4} P_i$, obtainable by using the qutrit state $\langle\psi| = (0, 0, 1)$. We find

$$\Sigma_q = \sum_{i=0}^{4} \mathrm{tr}\left(|\psi\rangle\langle\psi| P_i\right) = \sqrt{5} \approx 2.24. \tag{2.5}$$

Note that this is a state-dependent inequality, meaning that we only obtain a violation of the predictions of non-contextual hidden variable theories for subset of all possible states.

A violation of a KS inequality shows that certain non-contextual hidden variable models cannot accurately reproduce the outcomes of quantum mechanics. However, the hidden variable scheme we used above was influenced by quantum mechanics. When we forced the coin to only be present under at most one adjacent box, we were simulating the KS colouring rules, which are a direct consequence of the quantum mechanical formalism. This reliance on quantum mechanics can be removed by looking instead at correlation inequalities. Such inequalities, as their name suggests, involve averaging over measurements of two (or more) operators. The KS colouring rules are abandoned completely and the hidden variables are constrained only by the assumption of non-contextuality.

The 5 vectors from the KS inequality can also be used to construct a correlation inequality [27]. It is convenient to define the operators

$$A_i = 2P_i - \mathbb{1} \tag{2.6}$$

with spectra $\{-1, -1, 1\}$. Now, instead of assigning either of the truth values 0 or 1 to the vectors, we assign the variables $a_i = \pm 1$. In the hidden variable model, there are no restrictions on the assignments and we can perform all possible 2^5 of them to obtain a bound. Note that each vector in the pentagram appears in two different contexts. The correlation inequality is then formed from looking at joint measurements of the A_i operators in every context. For a non-contextual hidden variable model we find

$$\kappa_c = \sum_{i=0}^{4} \langle A_i A_{i+1} \rangle \geq -3, \tag{2.7}$$

where, as before, addition is modulo 5. The lower bound is saturated when there are two -1 assignments given to vertices not linked by a line in Figure (2.5). Although we relaxed the KS colouring rules, the switch from single to joint measurements penalises any hidden variable assignments that violate the principle of exclusiveness among operators. Again, we need to make the assumption that taking an average over many different ensembles is a fair reflection of all the assignments, and does not hide some deeper assignment properties. The quantum mechanical average, calculated using the same qutrit state as before, is

$$\kappa_q = \sum_{i=0}^{4} \mathrm{tr}\left(|\psi\rangle\langle\psi| A_i A_{i+1}\right) = 5 - 4\sqrt{5} \approx -3.94, \tag{2.8}$$

which violates the correlation inequality for a non-contextual hidden variable model.

Any set of vectors providing a KS proof produces a correlation inequality [28]. Translating the KS theorem in this way has allowed several experimental verifications of inequalities, both of the KS [9, 24, 25] and correlation variety [9].

2.2 Colourability

In the spirit of an evolving KS theorem, let us mention a very recent development. Traditionally, KS proofs were comprised of sets of vectors that are uncolourable following the KS rules. In 2012, Yu and Oh found a colourable set of vectors in $\mathbb{R}^3$ that forms a correlation inequality and also a KS inequality using a subset of four vectors [6]. We will denote such sets, whose vectors are colourable but give rise to inequalities, contextuality sets. The explicit vectors in the Yu and Oh contextuality set are shown in Table (2.1).

$$\begin{array}{cccc} (1,1,-1)^\intercal & (1,1,0)^\intercal & (1,-1,0)^\intercal & (1,0,0)^\intercal \\ (1,-1,1)^\intercal & (1,0,1)^\intercal & (1,0,-1)^\intercal & (0,1,0)^\intercal \\ (-1,1,1)^\intercal & (0,1,1)^\intercal & (0,1,-1)^\intercal & (0,0,1)^\intercal \\ (1,1,1)^\intercal & & & \end{array}.$$

Table 2.1: The 13 real vectors in the Yu and Oh set.

The thirteen vectors can be visualised as directions passing through the origin of a cube, as shown in Figure (2.6). The first column in Table (2.1) contains the four directions going through the vertices of the cube. The second and third columns are directions between the midpoints along two opposite edges, while the last column contains the three directions passing through the middle of the cube's faces.

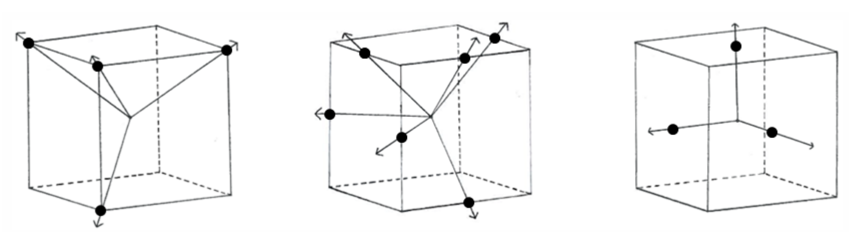

Figure 2.6: The directions of the 13 vectors in the Yu and Oh set. The first cube corresponds to vectors in the first column of Table (2.1), the second cube to the second and third columns, and the third cube to the fourth column.

The orthogonality graph for the Yu and Oh set is given in Figure (2.7). The standard basis vectors lie at the corners of the large triangle, while the vectors in the second and third columns in Table (2.1) form the smaller triangles connected to these. The remaining 4 vectors, from the first column in Table (2.1), are closest to the centre of the orthogonality graph.

Contrary to the examples in the previous section, both inequalities are state-independent, so a violation occurs for every qutrit state. We observe that for the inequalities to be state-independent, the sum of the projectors must be proportional to the identity. We can see this by looking at the

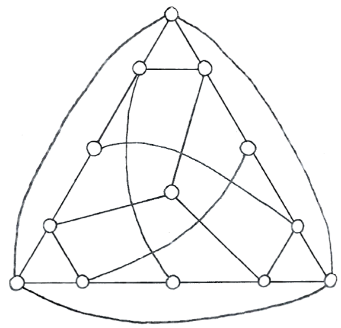

Figure 2.7: The orthogonality graph for the 13-vector set found by Yu and Oh.

quantum mechanical result of the KS inequality, which takes the form

$$\Sigma_q = \sum_{i=0}^{3} \mathrm{tr}\left(\rho P_i\right), \tag{2.9}$$

where the four projectors are formed from the vectors in the first column of Table (2.1). Calculating their sum gives

$$\sum_{i=0}^{3} P_i = \frac{4}{3}\mathbb{1}, \tag{2.10}$$

and so the KS inequality becomes

$$\Sigma_q = \sum_{i=0}^{3} \mathrm{tr}\left(\rho P_i\right) = \mathrm{tr}\left(\rho \sum_{i=0}^{3} P_i\right) = \frac{4}{3}\mathrm{tr}\left(\rho\right) = \frac{4}{3}. \tag{2.11}$$

Thus the state ρ can be any density matrix. A similar argument applies to the correlation inequality, given by

$$\kappa_q = \sum_{i=0}^{12} \mathrm{tr}\left(\rho A_i\right) - \frac{1}{2}\sum_{i,j}^{12} \Gamma_{ij}\mathrm{tr}\left(\rho A_i A_j\right), \tag{2.12}$$

where Γ_{ij} is the adjacency matrix, which takes the value 1 if vectors i and j are orthogonal and 0 otherwise. The relevant sums are

$$\sum_{i=0}^{12} A_i = \frac{13}{3}\mathbb{1} \quad \text{and} \quad \sum_{i,j}^{12} \Gamma_{ij} A_i A_j = -12\mathbb{1}. \tag{2.13}$$

Substituting these into the correlation inequality gives

$$\begin{aligned}\kappa_q &= \sum_{i=0}^{12} \mathrm{tr}\left(\rho A_i\right) - \frac{1}{2}\sum_{i,j}^{12} \Gamma_{ij}\mathrm{tr}\left(\rho A_i A_j\right) \\ &= \mathrm{tr}\left(\rho \sum_{i=0}^{12} A_i\right) - \frac{1}{2}\mathrm{tr}\left(\rho \sum_{i,j}^{12} \Gamma_{ij} A_i A_j\right) \\ &= \frac{25}{3}\mathrm{tr}\left(\rho\right) = \frac{25}{3}. \end{aligned} \tag{2.14}$$

This condition of projectors summing to the identity forms a central idea in quantum mechanics. Such sets are called positive operator valued measures (POVMs) and we will discuss them further in the next chapter. The POVMs used here are actually quite special in themselves, but again, this is a consideration for later. In addition to the contextuality set discussed above, Paper I contains a set of 21 vectors, which we will call the BBC set, that forms both a state-independent KS and state-independent correlation inequality in $\mathbb{C}^3$. In some ways, the BBC set is a natural extension of the Yu and Oh one. Its explicit vectors, with $q = e^{\frac{2\pi i}{3}}$, are given in Table 2.2.

$(0,1,-1)^\intercal$	$(0,1,-q)^\intercal$	$(0,1,-q^2)^\intercal$
$(-1,0,1)^\intercal$	$(-q,0,1)^\intercal$	$(-q^2,0,1)^\intercal$
$(1,-1,0)^\intercal$	$(1,-q,0)^\intercal$	$(1,-q^2,0)^\intercal$
$(1,0,0)^\intercal$	$(0,1,0)^\intercal$	$(0,0,1)^\intercal$
$(1,1,1)^\intercal$	$(1,q,q^2)^\intercal$	$(1,q^2,q)^\intercal$
$(1,q^2,q^2)^\intercal$	$(q^2,1,q^2)^\intercal$	$(q^2,q^2,1)^\intercal$
$(1,q,q)^\intercal$	$(q,1,q,)^\intercal$	$(q,q,1)^\intercal$

Table 2.2: The 21 complex vectors in the BBC set.

We shall quickly go through the inequalities for the BBC set. The KS inequality is obtained by summing the truth values, T_i, of the projectors onto the nine upper-most vectors in Table (2.2). We find an upper limit for the prediction of any non-contextual hidden variable theory of

$$\Sigma_c = \sum_{i=0}^{8} \langle T_i \rangle \leq 2. \tag{2.15}$$

The quantum mechanical average, if the state of the system is ρ, is

$$\Sigma_q = \sum_{i=0}^{8} \mathrm{tr}\,(\rho P_i) = 3. \tag{2.16}$$

This is a relatively large violation of the KS inequality, namely 1 compared to $\frac{1}{3}$ for the Yu and Oh set (though, of course, more projectors are required). The correlation inequality is of the Yu and Oh form in Equation (2.14). To calculate the classical result, we form the 21 operators A_i from the 21 vectors. Again, we introduce the dichotomic hidden variables a_i that take the values ± 1. The correlation inequality is then

$$\kappa_c = \sum_{i=0}^{20} \langle A_i \rangle - \frac{1}{5} \sum_{i,j}^{21} \Gamma_{ij} \langle A_i A_j \rangle \leq \frac{63}{5}. \tag{2.17}$$

As before, Γ_{ij}, with $1 \leq i, j \leq 21$, is the adjacency matrix, which is equal to 1 for commuting and distinct A_i and A_j, and 0 otherwise. The quantum mechanical expectation value is given by

$$\kappa_q = \sum_{i=0}^{20} \mathrm{tr}\,(\rho A_i) - \frac{1}{5} \sum_{i,j}^{21} \Gamma_{ij} \mathrm{tr}\,(\rho A_i A_j) = \frac{67}{5}. \tag{2.18}$$

This is a clear violation of the prediction from non-contextual hidden variable models.

On the subject of extending sets, Yu and Oh's contextuality set is a subset of a previous KS set found by Peres [16]. The 33 vectors in Peres' proof are all real and, in fact, have been shown to be a special choice of a more general one-parameter family of uncolourable vectors [29]. Another choice of parameters recovers a unitarily inequivalent set found by Penrose [17] involving complex vectors. This is the only known KS proof to include parameters in its vectors, or, in other words, the only known KS set where the orthogonality relations are not enough to uniquely determine the vectors [30].

The full Peres set can be seen as directions in three interlocking cubes, shown in Figure (2.8). In a correctly chosen basis, they coincide exactly with the 3 cubes in Escher's famous waterfall print.

The 13 vectors from the Yu and Oh contextuality set all lie within one cube and the remaining vectors in the Peres set are obtained by rotating the initial cube. There is some degeneracy among the vectors because the standard basis appears in each of the three cubes, so we find a total number of $13 \times 3 - 3 - 3 = 33$ vectors from the interlocking cubes. This can be seen

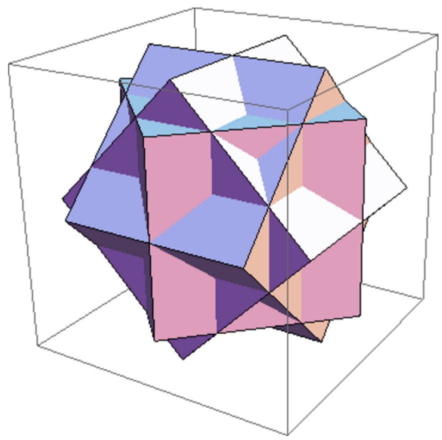

Figure 2.8: Three interlocking cubes that contain the 33 vectors in Peres' KS proof, one of which contains the 13 vectors in Yu and Oh's contextuality proof.

by comparing with the vectors in Figure (2.6), where the third cube appears in each individual cube in Figure (2.8). The vectors in the Yu and Oh set are completely determined by their orthogonalities, so the free parameter in the Peres set appears when we complexify the rotation matrix used to rotate the 13 vectors into the second and third cubes. On the orthogonality graph, this results in a few extra orthogonalities between the cubes, as shown in Figure (2.9).

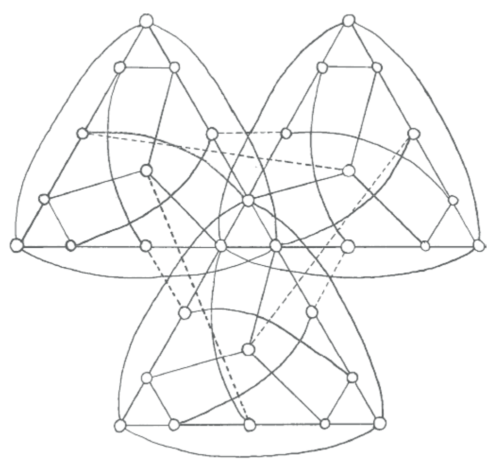

Figure 2.9: The orthogonality graph for the 33-vector set found by Peres. The dashed lines represent orthogonalities between the three cubes.

Developing KS and correlation inequalities from colourable sets of vectors shifts the role of the orthogonality graph. Traditionally in the KS theorem, the orthogonality graph was used to detect uncolourable sets of vectors, however, it can now be used for finding sets of vectors that violate inequalities of the type in Equation (2.17) [7]. Here, we call such sets a contextuality set or contextuality proof.

The Contextuality theorem. *For a set of vectors to produce a state independent contextuality proof, it must have an orthogonality graph with chromatic number $\chi(G)$ greater than the dimension N.*

The chromatic number of a graph is the fewest number of colours required to colour the graph such that all adjacent vertices have different colours. In the previous sections, the chromatic number for orthogonality graphs corresponding to KS proofs was always greater than 2.

Very recently, there have been two reported experimental implementations of the Yu and Oh contextuality inequality using trapped ions and a nitrogen-vacancy centre in diamond [10, 11]. In Paper II, we have given an explicit proposal both for an optimised inequality and a qutrit photon setup based on the Yu and Oh set. Furthermore, we have shown a direct relationship between the correlation inequality and a Bell inequality, which is relevant for criticisms of previous experimental procedures.

2.3 Configurations

Configurations are finite sets of points and lines with special intersection properties. They were studied extensively in the nineteenth century and formed a major area of geometry [14]. Before we discuss specific examples of configurations, we must decide where to house them; we shall consider both projective and affine spaces.

Affine space is a generalisation of Euclidean space; it is a set of points on which we can perform translations. If we equip affine space with an origin, we recover a vector space. Any affine plane obeys the following three axioms:

1. If p_α and p_β are distinct points, then there exists a line l_μ such that $p_\alpha, p_\beta \in l_\mu$. *Any two distinct points lie on a unique line.*

2. If $p_\alpha \notin l_\mu$, there is a unique line l_ν such that $p_\alpha \in l_\nu$ and $l_\mu \cap l_\nu = \emptyset$. *Given a point and a line not containing the point, there is at most one parallel line which contains the point.*

3. There exist at least three non-collinear points. *Trivial cases are excluded.*

A finite affine plane of order N is formed from a set of N^2 points and $N(N+1)$ lines. The lines can be collected into $N+1$ sets of N parallel lines, where parallel lines never meet and two non-parallel lines meet in exactly one point. It is known that finite affine planes exist when N is a prime or prime power, where we can assign coordinates to the points in the plane by using pairs of elements in the finite field $\mathbb{F}_N$. For some dimensions, such as $N = 6$, it is known that finite affine planes do not exist [31], while for others, such as $N = 12$, the question of existence is still open.

We are particularly interested in the finite affine plane of order 3, known as the Hesse configuration. It contains nine points and twelve lines, which can be grouped into four sets of three parallel lines. Each set is called a striation of the plane and they are given in Figure (2.10). We denote the configuration $(9_4, 12_3)$ to show there are in total nine points, each lying in four distinct lines, and twelve lines, each passing through three distinct points. Note that this is actually $\left(N^2_{N+1}, N(N+1)_N\right)$ for $N = 3$.

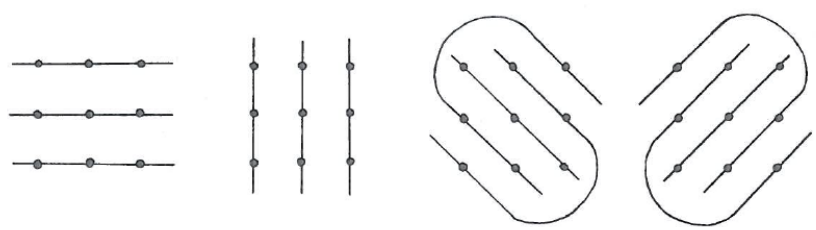

Figure 2.10: The four striations for the Hesse configuration in the finite affine plane. Each striation contains three parallel lines and each line contains three points.

Configurations in affine space are typically an abstract concept; there is no requirement of realisation. The Sylvester-Gallai theorem states that a finite collection of points in a projective plane are either all on a line, or else there is some line that contains exactly two of the points. As the Hesse configuration does not possess either of these properties, it cannot be reproduced using vectors in the Euclidean plane. However, it can be realised in the complex projective plane. The nine points are the inflection points of an elliptic curve—found by taking the Hessian of the cubic polynomial that defines the curve—and the lines are those that pass through these inflection points [32].

In some sense, the home of quantum information is complex projective space. Pure quantum states are technically rays in Hilbert space because we cannot physically distinguish between $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$, $\theta \in \mathbb{R}$. We also tend to normalise our vectors to have unit length and so remove another degree of freedom. All in all, when we talk about the state $|\psi\rangle$, we are really considering the equivalence relation of states

$$|\psi\rangle \sim \lambda|\psi\rangle \quad , \quad \lambda \in \mathbb{C}. \tag{2.19}$$

We define complex projective space, $\mathbb{C}P^{N-1}$, as the set of all 1-dimensional subspaces in $\mathbb{C}^N$. A projective point is then given by the homogeneous coordinates

$$(z^0, z^1, \ldots, z^{N-1}) \sim \lambda(z^0, z^1, \ldots, z^{N-1}), \quad \lambda \neq 0. \tag{2.20}$$

The language of projective space, like Euclidean space, is points, lines and planes. In the same way that a projective point is a 1-dimensional subspace of $\mathbb{C}^N$, a projective line is defined as a 2-dimensional subspace of $\mathbb{C}^N$, and so on. We will be largely concerned with 2-dimensional projective geometry, which, like incidence geometry, deals with the intersection of points, lines and planes. Any projective plane obeys the following three axioms:

1. If p_α and p_β are distinct points, then there exists a line l_μ such that $p_\alpha, p_\beta \in l_\mu$. *Any two distinct points lie on a unique line.*

2. The intersection of any two distinct lines contains exactly one point.

3. There exist at least three non-collinear points. *Trivial cases are excluded.*

A finite projective plane of order N contains a set of N^2+N+1 points and N^2+N+1 lines. Although the axioms are seemingly similar to those obeyed by the affine plane, there is a crucial difference in their treatment of parallel lines. In the affine case, parallel lines do not meet, but in the projective case every pair of lines intersects at one point and parallel lines meet at the "line at infinity." In fact, an affine plane can be obtained from a projective one by removing exactly one line (and the points on it).

We are more concerned with infinite projective spaces and, as an example, we can look at the real projective plane, $\mathbb{R}P^2$. It has the topology of the 2-sphere with antipodal points identified. A 1-dimensional subspace passing through the origin in $\mathbb{R}^3$ intersects the sphere at two antipodal points, both of which then correspond to one projective point. A 2-dimensional subspace passing through the origin in $\mathbb{R}^3$ intersects the sphere in a great circle, giving a projective line. We can see from inspection, shown in Figure (2.11), that two great circles meet at antipodal points on the sphere and, conversely, that two antipodal points lie on a great circle.

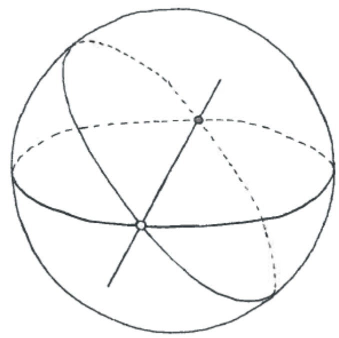

Figure 2.11: Projective points and lines in $\mathbb{R}P^2$. A line through the origin in $\mathbb{R}^3$ is a pair of antipodal points on the 2-sphere and a plane through the origin in $\mathbb{R}^3$ is a great circle.

This can be expanded to any dimension and we see that real projective space is equivalent to the quotient space

$$\mathbb{R}P^n = S^n/\mathbb{Z}_2, \tag{2.21}$$

where $n = N - 1$. A similar relation holds for complex projective space, namely

$$\mathbb{C}P^n = S^{2n+1}/S^1, \tag{2.22}$$

where S^{2n+1} is the set of all unit vectors in C^N and S^1 corresponds to the phase degree of freedom. Configurations in higher dimensions become sets of points, lines and planes.

If we look back at the axioms for the projective plane, we can see that interchanging the words "points" and "lines" leaves the axioms unchanged. This introduces the principle of duality in projective space, which states that every configuration in the projective plane has a dual in which the roles of points and lines are reversed. This also holds in higher dimensions, where points and $(N-1)$-dimensional subspaces are interchanged between two dual configurations.

Another famous configuration was introduced by Reye in the late nineteenth century. It consists of 12 points and 16 lines with the notation $(12_4, 16_3)$, meaning it has 12 lines each containing 4 points and 16 points each lying on 3 lines. It can be realised as the directions of a cube in $\mathbb{R}P^3$; an illustration of the configuration and its dual is given in Figure (2.12).

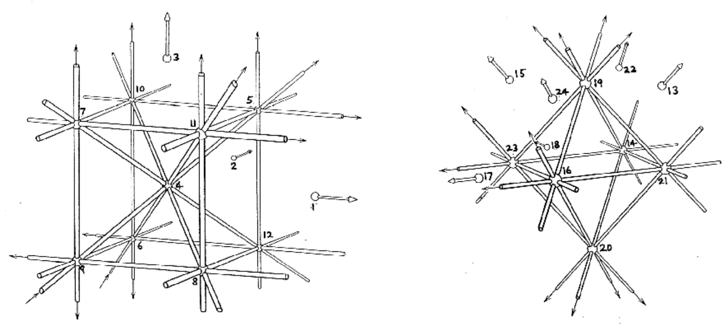

Figure 2.12: The Reye configuration (left) and its dual (right) in $\mathbb{R}P^3$. The points in one configuration are taken to be planes in the other. Image taken from *Geometry and the Imagination* by Hilbert and Cohn-Vossen [14].

The link to quantum theory is thus: the 24 points in the two Reye configurations in Figure (2.12) coincide with 24 vectors in a KS proof found by Peres [16]. The connection between the KS set and the configuration was shown by Aravind, who used it to explain many of the symmetries shown by the set and to construct a detailed argument for minimal uncolourable sets [34]. The explicit vectors in Peres' KS set are given in Table (2.3).

$(2,0,0,0)^\intercal$	$(0,2,0,0)^\intercal$	$(0,0,2,0)^\intercal$	$(0,0,0,2)^\intercal$
$(1,1,1,1)^\intercal$	$(1,-1,1,-1)^\intercal$	$(-1,-1,1,1)^\intercal$	$(1,-1,-1,1)^\intercal$
$(-1,-1,-1,1)^\intercal$	$(-1,1,1,1)^\intercal$	$(1,-1,1,1)^\intercal$	$(1,1,-1,1)^\intercal$
$(1,0,1,0)^\intercal$	$(0,1,0,1)^\intercal$	$(1,0,-1,0)^\intercal$	$(0,1,0,-1)^\intercal$
$(1,1,0,0)^\intercal$	$(1,-1,0,0)^\intercal$	$(0,0,1,1)^\intercal$	$(0,0,1,-1)^\intercal$
$(1,0,0,1)^\intercal$	$(0,1,1,0)^\intercal$	$(1,0,0,-1)^\intercal$	$(0,1,-1,0)^\intercal$

Table 2.3: The 33 vectors in the Peres KS set.

The connection to projective configurations also applies to contextuality proofs. The BBC set of 21 colourable vectors can be extracted from the Hesse configuration in $\mathbb{C}P^2$. The nine points correspond to the upper-most nine vectors in Table (2.2) while the lines correspond to the remaining 12 vectors; more specifically, the lines each produce a dual point and these points are the 12 vectors in Table (2.2). The whole Hesse configuration is shown in Figure (2.13), where it should be stressed that this is a picture of points and lines in the finite affine plane, not an orthogonality graph. We can see that it is just the four striations from Figure (2.10). We shall also use the Hesse configuration in the following section on symmetric measurements.

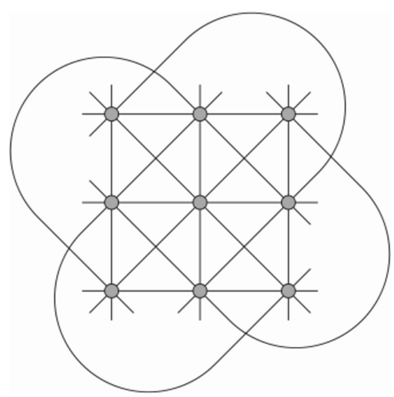

Figure 2.13: The Hesse configuration in $\mathbb{C}P^2$, where the curved and straight lines both indicate projective lines.

Chapter 3

Symmetric measurements

A generalised measurement in quantum theory is described using a positive operator valued measure (POVM). A POVM is a set of positive semi-definite operators, E_i, and we have already stated that they sum to the identity. Given these two conditions, a POVM, together with a density matrix, defines a probability distribution through the relation

$$p_i = \mathrm{Tr}(E_i \rho). \tag{3.1}$$

In general, this will be a restricted set of all possible probabilities on the outcome space, except in the case of idealised von Neumann measurements, where $E_i E_j = \delta_{ij} E_i$. Von Neumann measurements therefore correspond to vectors from an orthonormal basis and there can be at most N operators, while POVMs do not have an upper limit. The individual POVM elements are sub-normalised projectors, i.e. $E_i = \frac{1}{N}\Pi_i$ for projector $\Pi_i = |\psi_i\rangle\langle\psi_i|$.

A powerful result concerning POVMs is Naimark's dilation theorem, which states that every POVM can be thought of as a projective measurement on some larger, joint Hilbert space. There is a nice geometrical representation of this, formulated in the mid-twentieth century, known as Hadwiger's principal theorem. Let a star be a collection of k rays (or $2k$ vectors) passing through the origin in Hilbert space. It is called eutactic if it can be described as an orthogonal projection of a cross-polytope in $\mathbb{R}^k$. Hadwiger's theorem states that in order to obtain a eutactic star, the vectors must form a resolution of the identity in $\mathbb{R}^N$, i.e.

$$\sum_{i=0}^{k} |\phi_i\rangle\langle\phi_i| = \mathbb{1}. \tag{3.2}$$

This is precisely the condition for a POVM. A particular class of POVMs that we are interested in are called symmetric informationally-complete POVMs (SICs) [35]. To be informationally-complete, a POVM must have exactly N^2 elements—enough to completely determine the $N^2 - 1$ parameters in a general, unknown density matrix. The name symmetric comes from the restriction that the pairwise trace of the operators is always equal to a constant. We will work with rank 1 projectors satisfying the condition

$$\sum_{i=0}^{N^2-1} \Pi_i = \mathbb{1} \tag{3.3}$$

and

$$\mathrm{Tr}(\Pi_i \Pi_j) = \frac{1}{N+1} \quad i \neq j. \tag{3.4}$$

SICs are tomographically optimal in state reconstruction schemes [36] and are also used in quantum cryptography schemes [37]. Experimentally, they have been implemented in various tests in low dimensions [38, 39].

Once again, it is simpler to consider our projectors as vectors, in which case the SIC conditions become

$$\sum_{i=0}^{N^2-1} |\psi_i\rangle\langle\psi_i| = \mathbb{1}N \tag{3.5}$$

and

$$|\langle\psi_i|\psi_j\rangle|^2 = \frac{1}{N+1} \quad i \neq j. \tag{3.6}$$

It is worth mentioning a related concept here; mutually unbiased bases (MUBs) are also sets of vectors—this time collected into bases—with a constant squared inner product that obey the condition

$$|\langle\psi_i|\phi_j\rangle|^2 = \frac{1}{N}, \tag{3.7}$$

for the two orthonormal bases $\{|\psi_0\rangle, \ldots, |\psi_{N-1}\rangle\}$ and $\{|\phi_0\rangle, \ldots, |\phi_{N-1}\rangle\}$ [45]. The bases are said to be mutually unbiased because measuring with projectors from one basis tells you nothing about a system that has been prepared in the other basis. In other words, all outcomes occur with equal probability. This is the idea behind the famous Heisenberg uncertainty relation: if you know exactly where a particle is, you know nothing about its momentum. In this case, position and momentum are mutually unbiased.[1]

[1] The Heisenberg case uses an infinite-dimensional Hilbert space, whereas we restrict ourselves to a finite one here.

The maximum number of bases that can be mutually unbiased to a particular one is N [46], meaning the total number of independent outcomes from a complete set of MUBs is $N^2 - 1$. Notice that this is the same as for SICs, and so MUBs also offer an alternative tomographically efficient reconstruction scheme [48].

Armed with the definitions of SICs and MUBs, we can take another look at the configurations in the previous section. The explicit vectors in each of the two Reye configurations, given in Table (2.3), are the un-normalised vectors from a triplet of real MUBs. Each row is a basis and is unbiased with respect to the other two bases in the configuration. In 4 real dimensions, this is the maximum number of MUBs that can be found. Similarly, the 21 vectors in the Hesse configuration, given in Table (2.2), are a SIC (the uppermost 9 vectors) and a complete set of four MUBs (lower-most 12 vectors) in a three complex dimensional Hilbert space.

We claimed earlier that BBC vectors from the Hesse configuration were somehow an extension of the vectors in the Yu and Oh contextuality set. This is because the Yu and Oh vectors, Table (2.1), are an incomplete set of MUBs and SICs in a real 3-dimensional Hilbert space. The vectors in the first column in Table (2.1) are each unbiased to the computational basis in the fourth column. The middle two columns contain vectors that obey the SIC condition in Equations (3.5) and (3.6) and so each form one third of a full SIC.

3.1 Simplices

The set of all density matrices is a convex body in the (N^2-1)-dimensional real space of all unit trace Hermitian matrices. We can write an arbitrary density matrix as

$$\rho = \frac{1}{N}(\mathbb{1} + B), \tag{3.8}$$

where B is a Hermitian matrix of trace 0. We can then regard the set of traceless Hermitian matrices as a real vector space of dimension $N^2 - 1$, where the vector b corresponds to the matrix B. We denote this space as $\mathcal{D}$ and the convex set of all vectors corresponding to density matrices as the Bloch body, $\mathcal{B}$; in 2 dimensions $\mathcal{B}$ is the familiar Bloch ball.

To make any definite statements about the set of vectors in this space, we need a notion of distance. We use the re-scaled Hilbert-Schmidt inner product

$$\langle B_1, B_2 \rangle = \frac{1}{N(N-1)} \mathrm{Tr}(B_1 B_2). \tag{3.9}$$

The factor in front of the trace ensures the length of the vectors corresponding to density matrices equals 1, i.e. $||b|| = 1$, where the norm of a vector is defined as

$$||B|| = \sqrt{\langle B, B \rangle}. \tag{3.10}$$

To get an idea of what the SICs and MUBs look like in Bloch space, $\mathcal{D}$, we define two balls in this space with differing radii. The first is the largest ball centred on the origin that fits inside $\mathcal{B}$, given by

$$\mathcal{B}_o = \{b \in \mathcal{D} : ||b|| \leq 1\}. \tag{3.11}$$

The boundary of $\mathcal{B}_o$ is then the sphere

$$\mathcal{S}_o = \{b \in \mathcal{D} : ||b|| = 1\}. \tag{3.12}$$

All vectors corresponding to density matrices are contained within $\mathcal{S}_o$, although the converse is not true; not every vector in $\mathcal{S}_o$ corresponds to a density matrix and, in fact, only the points of this sphere that intersect with the Bloch body actually correspond to density matrices. Those that do are the pure states and they lie on a $2(N-1)$-dimensional sub-manifold of the Bloch body. Similarly, we define the smallest ball that encompasses $\mathcal{B}$ as

$$\mathcal{B}_i = \{b \in \mathcal{D} : ||b|| \leq \frac{1}{N-1}\}, \tag{3.13}$$

with the corresponding bounding sphere

$$\mathcal{S}_i = \{b \in \mathcal{D} : ||b|| = \frac{1}{N-1}\}. \tag{3.14}$$

$\mathcal{S}_i$ is in some ways the reverse of $\mathcal{S}_o$. Every vector in $\mathcal{S}_i$ corresponds to a density matrix, but not every density matrix is contained within $\mathcal{S}_i$.

A simplex in N dimensions is the convex hull (smallest convex set) spanned by $N+1$ extremal vectors. In the simplest case, $N = 1$, it is a line, for $N = 2$, a triangle, for $N = 3$, a tetrahedron, and so on. A SIC has N^2 projectors, or pure states, that are arranged equidistant from one another and so forms a regular simplex in $N^2 - 1$ dimensions. In Bloch space, the SIC problem becomes: can we fit a simplex in the Bloch body whose vertices lie on the manifold of pure states? It is easy to construct an (N^2-1)-dimensional simplex whose vertices lie on $\mathcal{S}_o$ (dimension $N^2 - 2$), but it is difficult to then rotate it so that the vectors lie on the manifold $\mathcal{B} \cap \mathcal{S}_o$ (dimension $2N - 2$).

All this becomes hard to visualise once $N > 2$, but we can look at the case for $N = 2$. The Bloch body is a 3-dimensional sphere and—uniquely—the balls $\mathcal{B}_o$ and $\mathcal{B}_i$ coincide. This means everything inside $\mathcal{S}_o$ corresponds to a possible density matrix and the Bloch body itself is a ball. Furthermore, the pure states cover the entire surface of $\mathcal{S}_o$ and we recover the familiar Bloch sphere. The SIC simplex, then, has its vectors lying on any point on the Bloch ball, as shown in Figure (3.1).

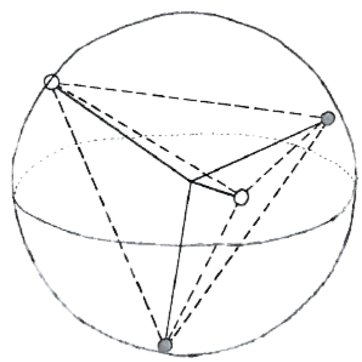

Figure 3.1: A SIC in 2 dimensions forms a regular tetrahedron with its four vertices lying on the Bloch sphere.

A similar argument applies to MUBs. An orthonormal basis corresponds to an $(N-1)$-dimensional regular simplex in $\mathcal{D}$. As with the SIC, it must be fully contained within the Bloch body, with all of its vertices lying on $\mathcal{S}_o$. A set of MUBs, then, is a collection of $N+1$ such simplices arranged as a regular polytope. We end up in a similar situation for the MUB problem: can we fit such a polytope in the Bloch body whose vertices lie on the manifold of pure states?

Turning again to $N = 2$, we can see from Figure (3.2) that the co-ordinate axes of the Bloch ball give three mutually unbiased bases. The MUB vectors form a polytope where each vector, like the SIC vectors, must lie on the Bloch sphere.

3.2 Searches

Given that the original definitions for SICs and MUBs were very easy to state, we might expect a similarly easy approach to finding them. However, they

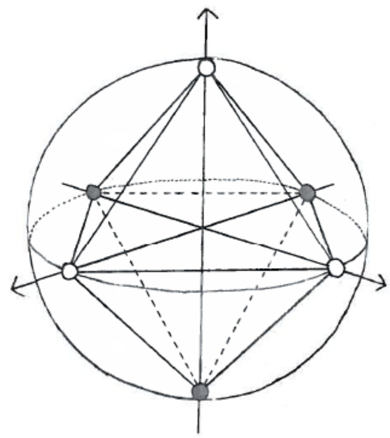

Figure 3.2: A MUB in 2 dimensions forms a regular polytope with its six vertices lying on the Bloch sphere.

are notoriously elusive—being either tricky to construct in some dimensions (SICs) or apparently lacking altogether in others (MUBs)—and a significant amount of research is focused on their existence. Published results have calculated SICs numerically in dimensions $N \leq 67$ [40]. MUBs are known to exist in prime and prime power dimensions [46] and a considerable amount of research suggests that a complete set of 7 MUBs cannot be found in $N = 6$ (the smallest composite dimension) [51]. Here we shall look at the constructions of both SICs and MUBs.

First, let us take a quick group theory tour. The Heisenberg-Weyl (HW) group is integral to both the SIC and the MUB problem and has a representation as upper-triangular matrices

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.15}$$

We are interested in the case when the matrix elements a, b and c are integers modulo N. The generators of the group are Z and X, which obey

$$ZX = \omega XZ \text{ and } X^N = Z^N = 1 \tag{3.16}$$

where $\omega = e^{\frac{2\pi i}{N}}$. We choose the representation

$$Z\,|r\rangle = \omega^r\,|r\rangle \ , \qquad X\,|r\rangle = |r+1\rangle \tag{3.17}$$

where all addition is modulo N. It is unique up to unitary equivalence. In $N = 2$, the operators X and Z are just the familiar Pauli spin matrices. It turns out to be convenient to define the phase factor

$$\tau = -e^{\frac{i\pi}{N}} \ , \qquad \tau^2 = \omega \ , \tag{3.18}$$

and introduce a vector $\mathbf{p}$ with integer entries. Then a general HW group element can be written as $\tau^{\kappa} D_{\mathbf{p}}$, where

$$D_{\mathbf{p}} = \tau^{ij} X^i Z^j \ , \qquad \mathbf{p} = \begin{pmatrix} i \\ j \end{pmatrix} \in \mathbb{Z}^2 \ . \tag{3.19}$$

With this notation, we can see that the following relations hold

$$D_{\mathbf{p}} D_{\mathbf{p}'} = \tau^{ij'-ji'} D_{\mathbf{p}+\mathbf{p}'} \ , \qquad D_{\mathbf{p}}^{\dagger} = D_{-\mathbf{p}} \ . \tag{3.20}$$

Note that τ is an N^{th} root of unity only in odd dimensions N; there are some unavoidable complications in even dimensions. The HW group modulo its centre is equal to the abelian group $Z_N \times Z_N$, which we can label with a square array of integers modulo N, and is called the HW collineation group. From now on we will always use this group, though we will often drop the term 'collineation' for brevity. An element of this group is specified by the vector $\mathbf{p}$, whose entries can be taken to be integers modulo N.

The construction of a complete set of MUBs in prime dimensions is straightforward [48]. The HW group contains $N+1$ non-overlapping abelian cyclic subgroups of order N, i.e. they all contain the identity element, but have no other element in common. We can check that this gives the correct number of operators in the group: $(N+1)(N-1)+1 = N^2$. The eigenbases of each subgroup are then mutually unbiased with respect to each other. In this way, we find $N+1$ MUBs. We can look at the simple example when $N = 2$. The HW group consists of the operators $\mathbb{1}$, σ_x, σ_z and $\sigma_x\sigma_z$. They form three trivial subgroups and we can construct three MUBs from their eigenbases:

$$\begin{aligned}
\{\mathbb{1}, \sigma_z\} \quad &\rightarrow \quad \{|0\rangle, |1\rangle\} \qquad\qquad (3.21)\\
\{\mathbb{1}, \sigma_x\} \quad &\rightarrow \quad \{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\} \equiv \{|+\rangle, |-\rangle\}\\
\{\mathbb{1}, \sigma_x\sigma_z\} \quad &\rightarrow \quad \{\frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}}\} \equiv \{|L\rangle, |R\rangle\}.
\end{aligned}$$

Referring back to Figure (3.2), we can see that the bases are precisely these axes in the Bloch sphere. It is clear that each basis has the same overlap with the other two and thus are mutually unbiased. This construction fails for composite dimensions because we cannot divide the HW group into such non-overlapping cyclic subgroups. In these dimensions, we can construct at least 3 MUBs this way.

For prime power dimensions, a similar procedure can be employed to generate $N+1$ MUBs [46]. However, instead of using the operators X and Z as defined in Equation (3.17), we modify them using elements in the Galois field—specifically, we let the elements a, b and c from Equation (3.15) belong to a Galois field. There are then $N+1$ sets of commuting operators, which each provide a basis that is mutually unbiased to the others. Again, we find $N+1$ MUBs.

In prime and prime power dimensions, there are additional ways to create MUBs from the orbits of the HW group, as discussed in Paper III.

The construction of SICs is somewhat more involved. It relies on two conjectures made by Zauner in his PhD thesis: (i) that SICs are group covariant, and (ii) that a fiducial vector in the SIC is invariant under an order 3 unitary matrix in the Clifford group [41]. Group covariance means that the SIC is an orbit under the action of a group and can therefore be generated by acting with every group element on one fiducial SIC vector. The group must have N^2 elements, which the HW collineation group has, and if the dimension is a prime it has been shown that the HW group is the only possible choice [43]. The vast majority of SICs are covariant with respect to the HW group, with only one known exception [44]. For the second conjecture, often referred to as Zauner invariance, we need to introduce the Clifford group.

The Clifford group is the normaliser of the HW group within the unitary group $U(N)$, and so it contains all unitary matrices U such that

$$UD_{\mathbf{p}}U^{\dagger} = \tau^{k}D_{\mathbf{p}'} \ . \tag{3.22}$$

Its action on the HW collineation group includes that of the symplectic group $SL(2, \mathbb{Z}_N)$, consisting of matrices

$$\mathcal{G} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} , \qquad \alpha\delta - \beta\gamma = 1 \bmod N \ , \tag{3.23}$$

where the entries are integers modulo N. We can convert between the two representations using

$$U_{\mathcal{G}} = \frac{e^{i\theta}}{\sqrt{N}} \sum_{k,l=0}^{N-1} |k\rangle \tau^{\beta^{-1}(\delta k^2 - 2kl + \alpha l^2)} \langle l| \ , \tag{3.24}$$

where θ is not determined by Equation (3.22). An additional step is needed if β does not have an inverse using arithmetic modulo N in odd dimensions and $2N$ in even dimensions [42]. Of course the Clifford group also includes the HW group itself as a subgroup. In odd dimensions, the Clifford group modulo its centre is isomorphic to a semi-direct product of $SL(2,\mathbb{Z}_N)$ with the HW collineation group. In even dimensions, the description is slightly more complicated [42]. However, although we will be concerned with even dimensions later, we will not expand on this here.

To use the Zauner invariance of SICs, we need to know the form of the order 3 unitary that the SIC is supposed to be invariant under. There are multiple order 3 unitary matrices in $U(N)$, and it is not difficult to check that these correspond to the matrices in $SL(2,\mathbb{Z}_N)$ if and only if they have trace -1, mod N. We will stick to the canonical choice

$$\mathcal{Z} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} , \tag{3.25}$$

unless otherwise stated [42]. We shall refer to the unitary matrix, $U_{\mathcal{Z}}$, corresponding to the symplectic matrix in Equation (3.25) as *the* Zauner unitary, and the other order 3 choices as Zauner unitaries. The phase θ in Equation (3.24) can then be found from the order three condition, $U_{\mathcal{Z}}^3 = \mathbb{1}$. This calculation requires a trigonometric sum that can be derived from a theta function identity [41]. The action of the Zauner unitary on the collineation group is

$$U_{\mathcal{Z}} D_{\mathbf{p}} U_{\mathcal{Z}}^{\dagger} = D_{\mathcal{Z}\mathbf{p}} \ . \tag{3.26}$$

The canonical choice of the symplectic matrix $\mathcal{Z}$ gives a unitary representation of $U_{\mathcal{Z}}$ with spectrum $\{1, q, q^2\}$. We denote the three corresponding eigenspaces as $\mathcal{H}_1$, $\mathcal{H}_q$ and $\mathcal{H}_{q^2}$, and give their dimensions in Table (3.1) [41]. There is still some freedom here as we can multiply by overall factors of q, but we shall keep to the subspaces shown here. Zauner's conjecture means that we expect to find a SIC fiducial vector in $\mathcal{H}_1$.

	$N = 3k$	$N = 3k+1$	$N = 3k+2$
1	$k+1$	$k+1$	$k+1$
q	k	k	$k+1$
q^2	$k-1$	k	k

Table 3.1: Multiplicities of the eigenvalues of $U_{\mathcal{Z}}$ for different dimensions.

As well as the Zauner matrix, the symplectic group contains HW translates of the Zauner matrix, which have the form $D_{\mathbf{p}} U_{\mathcal{Z}} D_{\mathbf{p}}^{\dagger}$.

Let's look again at our example of a SIC in $N = 2$. Returning to Figure (3.1), we can now see that the four SIC vectors are the orbit under the action of the HW group on some fiducial vector (it doesn't matter which vector we choose to be our fiducial): acting with X, Z or XZ permutes the SIC vectors. The Clifford group in 2 dimensions has order 24 and is isomorphic to the symmetry group of the cube. The order of the stability group of the fiducial vector—the group containing elements that leave the fiducial invariant—in the Clifford group is 3. This means there are eight distinct elements in a Clifford group orbit, corresponding to eight SIC vectors. We know a SIC in dimension 2 has four vectors, so we are left with two SICs. This is shown in Figure (3.3), where the two SICs are the two tetrahedra. The Clifford group permutes the fiducial vector, labelled $|\psi_0\rangle$, to the other vertices of the cube. The HW group permutes the vectors within the same SIC and the Zauner unitary rotates the vector along the axis of the fiducial vector, so the three other SIC vectors are permuted among themselves but $|\psi_0\rangle$ is left unchanged.

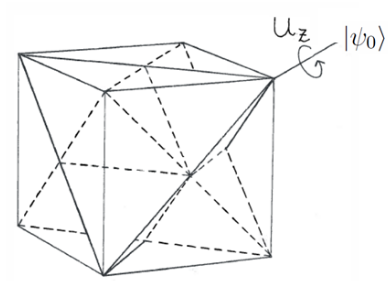

Figure 3.3: The action of the Clifford group on a SIC for $N = 2$. The SIC fiducial is invariant under the Zauner unitary, while other Clifford elements permute the SIC vectors between two distinct SICs.

In dimension 2 then, there are two SICs lying on a single Clifford group orbit. We can ask how the SICs are arranged with respect to the extended Clifford group—the group containing all unitary and anti-unitary transformations. It turns out that there are again two SICs on a single extended Clifford orbit, but this is unusual. In higher dimensions, the number of SICs on these orbits differs and we use the extended Clifford group to characterise SICs into orbits [42].

3.3 Subspaces

Let us return to the Hesse configuration. We know that the nine points correspond to SIC vectors and the 12 lines to a complete set of four MUBs. The lines correspond to 2-dimensional subspaces in $\mathbb{C}P^2$, where each subspace contains three SIC vectors. In other words, the SIC can be collected into linearly dependent sets of three vectors. The twelve lines in the Hesse configuration (see Figure (2.13)) give twelve such linearly dependent sets.

We can collect the 12 sets of dependent SIC vectors into orbits under the HW group. Naively, we might expect the sets to form a single orbit, but in fact they form four orbits, each containing only three sets.

In dimension 3, there is a continuous family of SICs parametrised by the real number t,

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -e^{i2t} \end{pmatrix}. \tag{3.27}$$

This is the only known dimension in which this happens. The SIC in our KS set from the previous section has $t = 0$, but the values $t = \frac{2\pi s}{9}$ for integer s also produce same the pattern of linear dependencies. Every other SIC in dimension 3 exhibits only three sets of three linearly dependent vectors. Paper III shows that these special nine SICs correspond to nine MUBs. We thus find 9 copies of the Hesse configuration in dimension 3.

A picture of the Hesse configuration in terms of the SIC and MUB vectors is given in Figure (3.4). Every vector in $\mathbb{C}P^2$ can be expressed as

$$\psi = \begin{pmatrix} \sqrt{p_0} \\ \sqrt{p_1}e^{i\nu_1} \\ \sqrt{p_2}e^{i\nu_2} \end{pmatrix} \quad , \quad p_0 + p_1 + p_2 = 1, \tag{3.28}$$

where the position in the simplex is determined by the parameters p_0, p_1 and p_2. Each point in the simplex has the topology of a torus, parametrised by the real numbers ν_1 and ν_2. This reduces to a circle with only one parameter along each edge. The MUB coming from the computational basis is given by the vertices of the simplex. The remaining MUBs lie on the torus at the very centre of the simplex, shown on the right-hand side of Figure (3.4). Each symbol on the torus corresponds to a vector from a particular MUB. The edges of the simplex are actually Bloch spheres and three SIC vectors lie in each Bloch sphere. They are linearly dependent and so lie on a great circle. This gives the usual set of three linear dependencies in every SIC; the nine additional dependencies are between one SIC vector from each sphere.

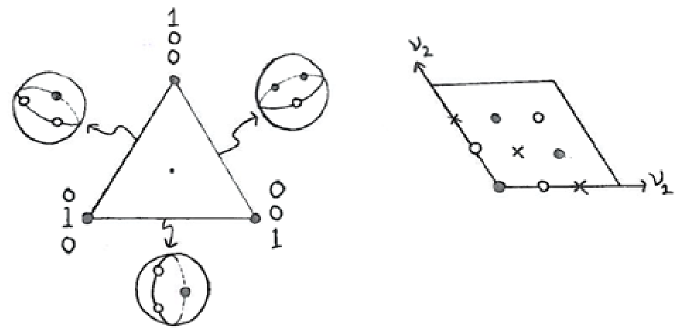

Figure 3.4: The SIC and MUB vectors in the Hesse configuration in the simplex.

A natural question is what happens in higher dimensions and the remainder of this section is dedicated to answering this [52]. For $N = 4$ and 5, there are no linear dependencies among SIC vectors, but for $N = 6$, they again appear. We will go on to show that the SIC linear dependency relations generalise in dimensions divisible by 3, and the SICs form just a small portion of the full linear dependency structure coming from the HW and Clifford groups. However, for now let us look at the dimension 6 case in more detail.

There is effectively only one SIC in dimension 6, insofar as all other SICs can be obtained from it by acting with the extended Clifford group, and it is given fully in [40]. A computer search for sets of 6 linearly dependent vectors reveals 984 such sets, where each of the 36 SIC vectors lies in 164 different sets. In a direct analogy to the Hesse configuration for dimension 3, we find the balanced configuration $(36_{164}, 984_6)$ in $\mathbb{C}P^5$.

The 984 sets divide up into orbits under the HW group. We find 27 orbits of length 36 and one orbit of length 12. The shorter orbit arises because it contains only linearly dependent sets invariant under the subgroup $\{\mathbb{1}, X^2Z^4, X^4Z^2\}$. This subgroup commutes with the Zauner unitary defined in Equations (3.25) and (3.24), which leaves the fiducial SIC vector invariant. Additionally, the sets in 22 of the HW orbits are invariant under the Zauner unitary or a HW translate of the Zauner unitary, i.e. the action of $D_pU_{\mathcal{Z}}D_p^\dagger$ on a set simply permutes its 6 vectors and leaves the overall set unchanged. However, there are 6 HW orbits whose sets are not invariant under $U_{\mathcal{Z}}$, but rather an order 6 unitary matrix.

Inspired by the dimension 3 case, we can calculate the unique vector that lies perpendicularly to each of the 984 5-dimensional subspaces formed from the linearly dependent sets. This gives us 984 “normal vectors". Performing an exhaustive search among these vectors does not reveal a basis—and certainly not seven mutually unbiased ones—but there are smaller groups of mutually orthogonal vectors. Specifically, we find that one of the orbits under the HW group splits into 9 sets of 4 mutually orthogonal vectors, which is as close to a basis as things come when $N = 6$.

There is further structure to be found among the 984 normal vectors. Instead of searching for inner products that vanish, we can look for inner products that square to $1/3$. There are 30 groups of 4 normal vectors whose mutual inner products that satisfy this condition and each group lies in 2-dimensional subspaces of the 6-dimensional Hilbert space. In other words, we have found 2-dimensional SICs within the linear dependency structure of a 6-dimensional SIC. The vectors all come from only 4 HW orbits, including the shorter one of length 12. More detail, including a recipe for finding these smaller dimensional SICs in dimension 6, will be found in [52].

Though this structure tells us about the interplay between the HW group and the subspaces of the Zauner unitary matrix, it is less informative on the subject of SICs. The structure we have detailed above is not dependent on SICs; if we look for linear dependencies among any orbit under the HW group when the fiducial vector belongs to $\mathcal{H}_1$, we recover the same 984 set linear dependency pattern. Had the linear dependencies only arisen for SICs, it could have opened new avenues into the SIC existence problem and may have helped to find them without the need for large, complex computer programs.

However, though the pattern of linear dependencies is identical for orbits with a fiducial vector in the Zauner subspace, regardless of whether the fiducial vector is in a SIC or not, there are some properties that are in fact SIC-specific. The 9 sets of 4 mutually orthogonal vectors only appear when we use a SIC vector to generate the linear dependencies. Over 200 additional orthogonalities between normal vectors also require a SIC fiducial. Thus the polytope formed from all the normal vectors is squashed when we replace the SIC fiducial with a random vector from $\mathcal{H}_1$.

A quick pictorial summary of these results in given in Figure (3.5). It is supposed to show the following steps: a vector was selected from the Zauner subspace $\mathcal{H}_1$, which was sometimes a SIC fiducial and sometimes not. Acting with the HW group produces an orbit of 36 vectors, in which we searched for linear dependencies. The resulting 984 dependencies collected into 28 HW orbits and consequently determined 984 normal vectors. The distances between these normal vectors were investigated: some normal vectors were orthogonal only for SIC linear dependencies and some normal vectors formed 2-dimensional SICs regardless of whether the original HW orbit formed a SIC.

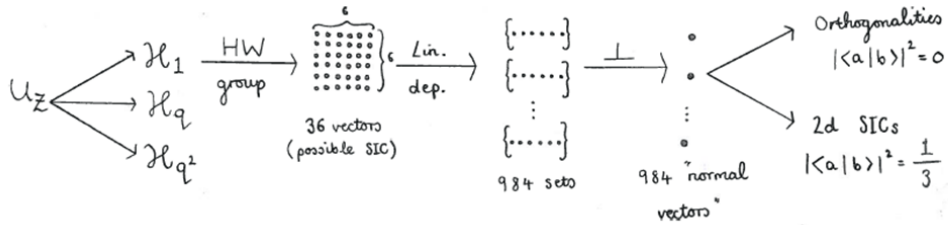

Figure 3.5: A summary of the linear dependencies among HW orbits, leading to SIC-specific orthogonality relations and 2-dimensional SICs.

Similar calculations have been made in dimensions 8 and 9 [52], where more dependencies were found. In dimension 9, there is a very large number of linear dependencies among the 81 SIC vectors, or, alternatively, among the 81 vectors in a HW orbit of a fiducial in the Zauner subspace. The configuration this produces is balanced and can be denoted $(81_{8,863}, 79, 767_9)$ in $\mathbb{C}P^8$. Again, 3-dimensional SICs were found among the normal vectors.

The link between projective geometry and SICs in dimension 3 gave rise to the famous Hesse configuration and something similar can be generalised to higher dimensions. However, it turns out that it is not a special property of SICs—the Hesse configuration is a unique case—but rather a more general property of the interplay between certain elements of the Clifford and HW groups. Explicitly, linear dependencies arise between vectors in a HW orbit when the fiducial vector is invariant under an order m unitary and the dimension is divisible by m, for $m = 2, 3$. In dimensions where $m = 3$, this coincides with finding linear dependencies among SIC vectors as the SIC fiducial is invariant under the order 3 Zauner unitary. We shall outline the argument here, starting with dimensions divisible by 3 and then expanding to dimensions divisible by 2.

The Linear Dependency theorem (dimensions divisible by 3). *In dimension $N = 3k$, any subset of N vectors in a HW orbit whose fiducial vector lies in the Zauner subspace $\mathcal{H}_1$ is linearly dependent if it is invariant under the action of $U_{\mathcal{Z}}$ or a HW translate of $U_{\mathcal{Z}}$.*

Proof. Let $N = 3k$. We require a fiducial vector invariant under the order three unitary $U_{\mathcal{Z}}$, i.e. satisfying $U_{\mathcal{Z}}|\psi_0\rangle = |\psi_0\rangle$, or under one of its Heisenberg translates, from which we construct three new linear combinations of vectors. Note that $|\psi_0\rangle$ need not be a SIC vector.

Our vectors are

$$|r\rangle = D_{\mathbf{p}}|\psi_0\rangle + U_{\mathcal{Z}} D_{\mathbf{p}}|\psi_0\rangle + U_{\mathcal{Z}}^2 D_{\mathbf{p}}|\psi_0\rangle$$

$$\begin{aligned} |s\rangle &= D_{\mathbf{p}} |\psi_0\rangle + q^2 U_{\mathcal{Z}} D_{\mathbf{p}} |\psi_0\rangle + q U_{\mathcal{Z}}^2 D_{\mathbf{p}} |\psi_0\rangle \\ |t\rangle &= D_{\mathbf{p}} |\psi_0\rangle + q U_{\mathcal{Z}} D_{\mathbf{p}} |\psi_0\rangle + q^2 U_{\mathcal{Z}}^2 D_{\mathbf{p}} |\psi_0\rangle \end{aligned} \tag{3.29}$$

which, it is straightforward to check, are evenly distributed between the eigenspaces $\mathcal{H}_1$, $\mathcal{H}_q$ and $\mathcal{H}_{q^2}$, shown in Table (3.1). Each new vector is a sum of three vectors from a single HW orbit, as

$$U_{\mathcal{Z}} D_{\mathbf{p}} |\psi_0\rangle = U_{\mathcal{Z}} D_{\mathbf{p}} U_{\mathcal{Z}}^{\dagger} U_{\mathcal{Z}} |\psi_0\rangle = D_{\mathcal{Z}\mathbf{p}} |\psi_0\rangle \ , \tag{3.30}$$

where $D_{\mathcal{Z}\mathbf{p}}$ and $D_{\mathbf{p}}$ lie on the same orbit by construction. The same argument works for the terms involving the square of the Zauner unitary. It is clear that the linear span of the vectors $\{|r\rangle, |s\rangle, |t\rangle\}$ equals that of the vectors $\{D_{\mathbf{p}} |\psi_0\rangle, D_{\mathcal{Z}\mathbf{p}} |\psi_0\rangle, D_{\mathcal{Z}^2\mathbf{p}} |\psi_0\rangle\}$.

We can label a vector in a HW orbit, up to a phase, by a 2-component vector $\mathbf{p}$ in $\mathbb{Z}_N^2$. In this representation, we are interested in the orbit of $\mathbf{p}$ under the action of $\mathcal{Z}$. We note that if and only if the dimension is divisible by 3 there will be non-trivial fixed points under this action, namely

$$\mathcal{Z}\mathbf{p} = \mathbf{p} \quad \Leftrightarrow \quad \mathbf{p} \in \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} k \\ 2k \end{pmatrix}, \begin{pmatrix} 2k \\ k \end{pmatrix} \right\} \ , \tag{3.31}$$

If $\mathbf{p}$ is one of the fixed points of $\mathcal{Z}$, given by Equation (3.31), it will form a singlet, otherwise it forms a triplet. In order to find a set of N vectors that is invariant under $U_{\mathcal{Z}}$, we take k triplets or a combination of the 3 singlets and $k-1$ triplets and substitute them into Equation (3.29). This gives k-many of each r-, s- and t-type vector. From Table (3.1) we know that the r-type vectors lie in an eigenspace of dimension $k+1$, the s-type vectors in an eigenspace of dimension k, and the t-type vectors in an eigenspace of dimension $k-1$. It is clear then that the k r-type vectors cannot fully span their subspace while the k t-type vectors are over-complete and therefore linearly dependent. There are 3 vectors from a HW orbit in each t-type vector and we have used k of them, so we find a total of $3k = N$ vectors from a HW orbit that are linearly dependent. □

The assumption of Zauner-invariance of the set of N vectors in the above proof means that not all linearly dependent sets are found this way. In dimension 6, we previously noted there were 984 sets of 6 linearly dependent vectors in HW orbits, however the method outlined above finds only 768 of them. In other words, the 6 orbits that are not invariant under the Zauner unitary or one of its HW translates (each containing 36 sets) are not included in this theorem.

We now branch away from SICs to show that linear dependencies occur between vectors in a HW orbit when the fiducial vector is invariant under an order 2 unitary and the dimension is divisible by 2.

First, we need some preliminary information. The symplectic group $SL(2,\mathbb{Z}_N)$ has a unique element of order 2 that is invariant under conjugation by every other element on the group. It is given by

$$\mathcal{A} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} . \tag{3.32}$$

This transformation of the collineation group is effected by the unitary matrix

$$U_{\mathcal{A}} = \sum_{k,l} |k\rangle \delta_{0,k+l} \langle l| \ , \qquad U_{\mathcal{A}}^2 = \mathbf{1} \ , \tag{3.33}$$

$$U_{\mathcal{A}} D_{\mathbf{p}} U_{\mathcal{A}}^{\dagger} = D_{\mathcal{A}\mathbf{p}} \ . \tag{3.34}$$

(In odd prime dimensions $\mathcal{A}$ is known as a phase-point operator, introduced by Wootters in connection with MUBs [53].) This action has four non-trivial fixed points if the dimension is divisible by 2, given by

$$\mathcal{A}\mathbf{p} = \mathbf{p} \quad \Leftrightarrow \quad \mathbf{p} \in \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} k/2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ k/2 \end{pmatrix}, \begin{pmatrix} k/2 \\ k/2 \end{pmatrix} \right\} . \tag{3.35}$$

The eigenvalues of $\mathcal{A}$ are $\{+1,-1\}$ and we denote the two corresponding eigenspaces as $\mathcal{H}_+$ and $\mathcal{H}_-$, giving their dimensions in Table 3.

	$N = 2k$	$N = 2k+1$
1	$k+1$	$k+1$
-1	$k-1$	k

Table 3.2: Multiplicities of the eigenvalues of $U_{\mathcal{A}}$ for different dimensions.

The Linear Dependency theorem (dimensions divisible by 2). *In dimension $N = 2k$, subsets of N vectors in a HW orbit whose fiducial vector lies in the Zauner subspace $\mathcal{H}_+$ are linearly dependent if they are invariant under the action of $U_{\mathcal{A}}$ and if fewer than k of the vectors are individually invariant under $U_{\mathcal{A}}$.*

Proof. Let $N = 2k$. We require a fiducial vector invariant under the order two unitary $U_{\mathcal{A}}$, i.e. satisfying $U_{\mathcal{A}} |\psi_0\rangle = |\psi_0\rangle$, and prove that any subset of N vectors (within a HW orbit) that transforms into itself under $U_{\mathcal{A}}$ is linearly dependent.

We begin by constructing two new linear combinations of vectors

$$|u\rangle = D_{\mathbf{p}} |\psi_0\rangle + U_{\mathcal{A}} D_{\mathbf{p}} |\psi_0\rangle$$
$$|v\rangle = D_{\mathbf{p}} |\psi_0\rangle - U_{\mathcal{A}} D_{\mathbf{p}} |\psi_0\rangle \tag{3.36}$$

which lie in the subspaces $\mathcal{H}_+$ and $\mathcal{H}_-$, respectively, shown in Table (3.2). Again, each new vector is a sum of two vectors from a single HW orbit and the linear span of the vectors $\{|u\rangle, |v\rangle\}$ equals that of the vectors $\{D_{\mathbf{p}} |\psi_0\rangle, D_{\mathcal{A}\mathbf{p}} |\psi_0\rangle\}$.

We turn again to the orbits of $\mathbf{p}$ under the action of $\mathcal{A}$. If $\mathbf{p}$ is one of the fixed points of $\mathcal{A}$, given by Equation (3.35), it will form a singlet, otherwise it forms a doublet. Taking k such doubles and substituting them into the vectors in Equation (3.36) produces k new u- and v-type vectors. These lie in subspaces of dimension $k+1$ and $k-1$ respectively, and thus the k v-type vectors must be linearly dependent. This in turn forces the $2k = N$ vectors in the HW orbit that make up each v-type vector to be linearly dependent. At this point, there is a minor difference to the previous theorem for dimensions divisible by 3. Taking the two $\mathbf{p}$ singlets and $k-1$ doublets and substituting them into Equation (3.36) does not provide N linearly dependent vectors. □

We expect a construction similar to the ones given here to hold for other dimensions.[2] We are currently restricted to dimensions where we know the subspaces of the order N unitaries for dimensions divisible by N. For example, if we knew the spectra of the order 5 element of the Clifford group in dimensions $N = 5$, 25, 35, 55, etc. then we could evaluate whether a modified version of the above theorems would result in linear dependencies in HW orbits of a fiducial vector left invariant under the order 5 unitary.

[2] In fact, a result in this direction, though not given here, is expected to be published soon [52].

Chapter 4

Conclusion

The recent development in the Kochen-Specker theorem has renewed interest in contextuality, both as a fundamental principle of quantum theory and as an experimental test of quantum mechanics. We showed how it relates to the debate about hidden variables and effectively rules out a certain class of these, namely non-contextual hidden variable models. We also discussed the role of configurations in contextuality proofs and in Paper I we show how the BBC set (found from the points and lines in the Hesse configuration) can be used to construct state-independent KS and contextuality inequalities. A more experimentally-friendly version of such inequalities is given in Paper II using the Yu and Oh set of vectors.

Both of these sets contain special vectors: SICs and MUBs. While the Yu and Oh set includes incomplete MUBs and SIC vectors in 3 real dimensions, the BBC set utilises a complete SIC and four MUBs in 3 complex dimensions. The relation between the SIC and MUBs is captured by the Hesse configuration in the complex projective plane, where linear dependencies among the 9 SIC vectors generate the 12 MUB vectors. Paper III explores this idea further and expands the Hesse configuration to other SICs and MUBs.

Motivated by this pattern, we searched for linear dependencies in higher dimensional SICs. We did not find any analogous relationships between SICs and MUBs, but we did prove that in dimensions divisible by three, SIC vectors will always contain sets of N linearly dependent vectors. The calculations in dimension 6 and 9 show one large difference to the dimension 3 case: there are no special SICs with a higher number of linear dependencies than other SICs. In some sense, this makes the Hesse configuration in dimension 3 more remarkable.

Bibliography

[1] A. C. Elitzur and L. Vaidman, *Quantum mechanical interaction-free measurements* Found. Phys. **23** 987 (1993)

[2] J. Eisert, M. Wilkens and M. Lewenstein, *Quantum Games and Quantum Strategies* Phys. Rev. Lett. **83** 3077 (1999)

[3] A. Einstein, B. Podolsky and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev. **47** 777 (1935)

[4] J. Bell, *On the Einstein Podolsky Rosen Paradox* Physics **1** (3) 195 (1964)

[5] S. Kochen and E. P. Specker, *The Problem of Hidden Variables in Quantum Mechanics* J. Math. Mech. **17** 59 (1967)

[6] S. Yu and C. H. Oh, *State-independent proof of Kochen-Specker theorem with 13 rays* Phys. Rev. Lett. **108**, 030402 (2012)

[7] A. Cabello, *State-independent quantum contextuality and maximum nonlocality* arXiv:1112.5149v2 (2012)

[8] S. Abramsky and L. Hardy, *Logical Bell Inequalities* Phys. Rev. A **85** 062114 (2012)

[9] E. Amselem, M. Radmark, M. Bourennane and A. Cabello, *State-independent quantum contextuality with single photons* Phys. Rev. Lett. **103** 160405 (2009)

[10] X.-Y. Pan, G.-Q. Liu, Y.-C. Chang and H. Fan, *Room temperature state-independent experimental test of quantum contextuality in solid state system* arXiv:1209.2901v2 (2012)

[11] X. Zhang *et al.*, *State-independent experimental tests of quantum contextuality in a three dimensional system* arXiv:1209.3831v1 (2012)

[12] C. A. Fuchs and R. Schack, *Quantum-Bayesian Coherence* arXiv:0906.2187 (2009)

[13] G. Farmelo, *Dirac's hidden geometry* Nature **437** 323 (2005)

[14] D. Hilbert and S. Cohn-Vossen, *Geometry and the Imagination* Chelsea Publishing House (1952)

[15] Gleason, *Measures on the Closed Subspaces of a Hilbert Space* J. Math. Mech. **6** 885 (1957)

[16] A. Peres, *Two simple proofs of the Kochen-Specker theorem* Journ. Phys. A **24** 175 (1991)

[17] R. Penrose, *On Bell non-locality without probablities: some curious geometry* in Quantum Reflections, edited by J. Ellis and D. Amati, Cambridge University Press (2000)

[18] M. Kernaghan, *Bell-Kochen-Specker theorem for 20 vectors* J. Phys. A: Math. Gen **27** L829 (1994)

[19] J. H. Conway and S. Kochen, reported in A. Peres, *Quantum Theory: Concepts and Methods* Springer (1995)

[20] A. Cabello, J. Estebaranz and G. García-Alcaine, *Bell-Kochen-Specker theorem: A proof with 18 vectors* Phys. Lett. A **212** 183 (1996)

[21] M. Pavicic, J.-P. Merlet, B. D. McKay and N. D. Megill, *Kochen-Specker Vectors* J. Phys. A **38** 1577 (2005)

[22] P. Heywood and M. L. G. Redhead, *Nonlocality and the Kochen–Specker paradox* Found. Phys. **13** 481 (1982)

[23] A. Stairs, *Quantum logic and the Lüders rule* Phil. Sci. **50** 578 (1982)

[24] Y.-F. Huang et al, *Experimental Test of the Kochen-Specker Theorem with Single Photons* Phys. Rev. Lett. **90**, 250401 (2003)

[25] R. Łapkiewicz et al, *Experimental non-classicality of an indivisible quantum system*, Nature **474** 490 (2011)

[26] R. Wright, *The state of the pentagon* in A. R. Marlow, *Mathematical Foundations of Quantum Mechanics* Academic Press, New York (1978)

[27] A. A. Klyachko, M. A. Can, S. Binicioglu, and A. S. Shumovsky, *A simple test for hidden variables in spin-1 system* Phys. Rev. Lett. **101**, 020403 (2008)

[28] P. Badziag, I. Bengtsson, A. Cabello and I. Pitowsky, *Universality of state-independent violation of correlation inequalities for non-contextual theories* Phys. Rev. Lett. **103** 050401 (2009)

[29] E. Gould and P. K. Aravind, *Isomorphism between the Peres and Penrose proofs of the BKS theorem in three dimensions* Found. Phys. **40** 1096 (2010)

[30] K. Blanchfield, *How orthogonalities set Kochen-Specker sets* in G. Jaeger et al, *Advances in Quantum Theory* AIP Conf. Proc. **1327** (2011)

[31] R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes* Canadian J. Math. **1** 88 (1949)

[32] O. Hesse, *Uber die Wendepuncte der Curven dritter Ordnung* J. Reine Angew. Math. **28** 97 (1844)

[33] T. Reye, *Das Problem der Configurationen* Acta Mathematica **1** 93 (1882)

[34] P. K. Aravind, *How Reye's configuration helps in proving the Bell-Kochen-Specker theorem: a curious geometrical tale* Found. Phys. Lett. **13** 499 (2000)

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

[36] A. Scott, *Tight informationally complete quantum measurements* J. Phys. A **39** 13507 (2006)

[37] T. Durt, A. Lamas-Linares, A. Ling and C. Kurtsiefer, *Wigner tomography of two qubit states and quantum cryptography* Phys. Rev. A **78** 042338 (2008)

[38] J. Du, M. Sun, X. Peng and T. Durt, *Realization of entanglement-assisted qubit-covariant symmetric-informationally-complete positive-operator-valued measurements* Phys. Rev. A **74** 042341 (2006)

[39] Z. E. D. Medendorp, F. A. Torres-Ruiz, L. K. Shalm, G. N. M. Tabia, C. A. Fuchs and A. M. Steinberg, *Experimental characterization of qutrits using SIC-POVMs* Phys. Rev. A **83** 051801 (2011)

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

[41] G. Zauner, *Quantendesigns. Grundzuge einer nicht- kommutativen Designtheorie* PhD thesis, Univ. Wien (1999); English translation in Int. J. Quant. Inf. **9** 445 (2011)

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

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

[44] S. G. Hoggar, *64 lines from a quaternionic polytope* Geom. Dedic. **69** 287 (1998)

[45] J. Schwinger, *Unitary Operator Bases* Proc. Natl. Acad. Sci. U.S.A. **46** 570 (1960)

[46] W. K. Wootters and B. D. Fields, *Optimal state-determination by mutually unbiased measurements* Ann. Phys. **191** 363 (1989)

[47] A. Klappenecker and M. Rötteler, *Constructions of Mutually Unbiased Bases* arXiv:0309120 (2003)

[48] I. Ivanovic, *Geometrical description of quantal state determination* J. Phys. A **14** 3241 (1981)

[49] M. Wiesniak, T. Paterek and A. Zeilinger, *Entanglement in mutually unbiased bases* New Journal of Physics **13** 053047 (2011)

[50] L. Hughston, *d=3 SIC-POVMs and Elliptic Curves* seminar at Perimeter Institute, available online at http://pirsa.org/07100040/ (2007)

[51] P. Raynal, X. Lü and B.-G. Englert *Mutually unbiased bases in dimension six: The four most distant bases* Phys. Rev. A **83** 062303 (2011)

[52] H. B. Dang, K. Blanchfield, I. Bengtsson and D. M. Appleby, *Linear Dependencies in Heisenberg-Weyl orbits* to appear

[53] W. K. Wootters, *A Wigner-function formulation of finite-state quantum mechanics* Ann. Phys. **176** 1 (1987)