Order 3 Symmetry in the Clifford Hierarchy

Ingemar Bengtsson[1], Kate Blanchfield[1], Earl Campbell[2,3] and Mark Howard[4]

[1]*Stockholms universitet, Fysikum, S-106 91 Stockholm, Sweden*
[2]*Department of Physics and Astronomy, University of Sheffield, Sheffield, S3 7RH, UK*
[3]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, Berlin, Germany*
[4]*Institute for Quantum Computing and Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1*

Abstract

We investigate the action of the first three levels of the Clifford hierarchy on sets of mutually unbiased bases comprising the Ivanovic MUB and the Alltop MUBs. Vectors in the Alltop MUBs exhibit additional symmetries when the dimension is a prime number equal to 1 modulo 3 and thus the set of all Alltop vectors splits into three Clifford orbits. These vectors form configurations with so-called Zauner subspaces, eigenspaces of order 3 elements of the Clifford group highly relevant to the SIC problem. We identify Alltop vectors as the magic states that appear in the context of fault-tolerant universal quantum computing, wherein the appearance of distinct Clifford orbits implies a surprising inequivalence between some magic states.

1

1 Introduction

The Weyl-Heisenberg group, also known as the qudit Pauli group, is deeply interwoven with the very foundations of quantum mechanics [1]. The group of unitaries that map the Weyl-Heisenberg group to itself under conjugation is known as the Clifford group, and plays a major role in a theory of fault-tolerant quantum computation [2]. If the dimension of Hilbert space is a prime number, then a complete set of mutually unbiased bases (MUB) arises as an orbit of the Clifford group [3, 4]. The vectors in such a set are also known as stabilizer states because they are stabilized by (i.e. they are eigenvectors of) elements of the qudit Pauli group.

If a quantum computer is restricted to performing Clifford operations on the stabilizer states it cannot outperform its classical counterparts [5]. One way to achieve universal quantum computation is to introduce certain "magic" states for the quantum computer to act on [6, 7, 8, 9, 10, 11]. Such states can be obtained by acting on the stabilizer states with elements of the third level of the Clifford hierarchy, which consists of those unitaries that map the Weyl-Heisenberg group into the Clifford group [12]. When acting on the stabilizer states, a unitary at this third level turns the usual MUB into another MUB, which is itself an orbit of the Weyl-Heisenberg group with one extra basis appended [13, 14]. These are the magic states that we will discuss, under the name of Alltop vectors. In the qubit case they are also known as "H-type magic states" [6].

The purpose of this paper is to point out the peculiar role played by Clifford group elements of order 3 in this context whenever the dimension of Hilbert space is a prime $p = 1$ modulo 3. In this case each Alltop vector is invariant under such an order 3 element. What is more, the set of all Alltop vectors forms a configuration [15] together with the set of largest subspaces left invariant by these order 3 elements. For a reason that we will come to these subspaces are called Zauner subspaces, and the precise statement is that each Alltop vector belongs to p Zauner subspaces, and each Zauner subspace contains $2(p-1)$ Alltop vectors.

One consequence is that the set of these magic states splits into 3 distinct orbits under the Clifford group if the dimension is $p = 1$ modulo 3, while there is only one orbit if $p = 2$ modulo 3. This is of interest to the magic state model for fault-tolerant universal quantum computing. However, here our primary interest is a curious parallel between magic states and symmetric, informationally complete (SIC) measurements. The latter form what are

arguably the most distinguished of all Weyl-Heisenberg orbits. In dimension 2, the vectors in a SIC are also known as "T-type magic states" [6]. In a general dimension N, a SIC is a POVM consisting of N^2 unit vectors $|\psi_I\rangle$ obeying

$$|\langle \psi_I | \psi_J \rangle|^2 = \frac{1}{N+1} \tag{1}$$

whenever $I \neq J$ [16, 17]. With one exception, all known SICs are group covariant with respect to the Weyl-Heisenberg group and in prime dimensions this is the only group that could do the job [18]. It is an outstanding problem to prove that the Weyl-Heisenberg group produces SICs for all dimensions. The available evidence suggests that it does, but no constructive procedure is known [19, 20, 21].

Analytic examples of SICs are known in (at the moment) 23 different dimensions. For some utterly mysterious reason all known SIC vectors are left invariant by a Clifford group element of order 3, in agreement with a conjecture first made by Zauner [16]. Moreover it appears that every Zauner subspace contains at least one SIC vector [19, 20]. We now have a different line of argument singling out these subspaces for attention, and we suggest that this hints at a deeper connection between MUBs and SICs. Indeed, one weak link is already known [22, 23]. In dimension $p = 3$ there is a very direct link, effectively discovered by Hesse in a different language [24], and elaborated on since [25]. We believe that we have strengthened the case for such a link in dimensions of the form $p = 1$ modulo 3, and consequently these dimensions may be the most promising ones for solving the SIC existence problem.

We review some known facts—briefly, because they are well explained elsewhere—in sections 2 and 3. In section 4 we point out the special role that the order 3 symmetries play within the Clifford hierarchy when the dimension equals 1 modulo 3. In section 5 we explore the consequences. In particular we show that the Zauner subspaces and the magic vectors in the MUBs form configurations whenever the dimension $p = 1$ modulo 3. We will also show that in these dimensions the magic vectors form three distinct orbits under Clifford gates. There is only one orbit if $p = 2$ modulo 3. In section 6 we comment on the remarkable reality properties of the Alltop vectors. Section 7 describes the relationship of Alltop vectors to quantum computing. Section 8 gives a brief summary.

Unless otherwise stated we assume that the dimension of Hilbert space is a

prime number $p > 3$, since this obviates the need for complicated caveats. As a matter of fact MUBs work somewhat differently in prime power dimensions, and they may well not exist in dimensions not equal to a power of a prime while SICs presumably do.

2   The Clifford hierarchy

In prime dimensions there is an essentially unique unitary representation of the finite Weyl-Heisenberg group, generated by clock and shift operators

$$X|r\rangle = |r+1\rangle \ , \qquad Z|r\rangle = \omega^r |r\rangle \ , \qquad \omega \equiv e^{\frac{2\pi i}{p}} \ , \qquad (2)$$

where the kets are labelled by integers modulo p. It is convenient to describe this group using the vector $\mathbf{p} = (p_1, p_2)$ and the displacement operators [19]

$$D_{\mathbf{p}} = \omega^{\frac{p_1 p_2}{2}} X^{p_1} Z^{p_2} \ . \qquad (3)$$

We let $1/\beta$ denote the multiplicative inverse modulo p of the integer β. The Clifford group also includes a copy of the symplectic group $SL(2, \mathbb{Z}_p)$, whose defining representation consists of two by two matrices with entries that are integers modulo p and whose determinant equals unity. It is generated by the matrices

$$T = \left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \ , \qquad F = \left(\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right) \ . \qquad (4)$$

They will figure later on. With the representation of the Weyl-Heisenberg group already fixed, the unitary representation of the symplectic group is

$$G = \left(\begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right) \ \rightarrow \ \begin{cases} U_G = \frac{e^{i\theta}}{\sqrt{N}} \sum_{r,s} \omega^{\frac{1}{2\beta}(\delta r^2 - 2rs + \alpha s^2)} |r\rangle\langle s| & \beta \neq 0 \\[2ex] U_G = \pm \sum_s \omega^{\frac{\alpha\gamma}{2} s^2} |\alpha s\rangle\langle s| & \beta = 0 \ . \end{cases} \qquad (5)$$

These operators are known as symplectic unitaries. We ignore the overall phase factors except to note that a suitable choice of θ means the unitary U_G is of the same order as G. In fact, they can be chosen so that the unitary

representation is faithful [26]. The full Clifford group contains products of Weyl-Heisenberg and symplectic unitaries.

With the above definitions one finds

$$D_{\mathbf{p}}D_{\mathbf{q}} = \omega^{q_1 p_2 - q_2 p_1} D_{\mathbf{p}+\mathbf{q}} , \qquad U_G D_{\mathbf{p}} U_G^{-1} = D_{G\mathbf{p}} . \tag{6}$$

A general element of the Clifford group can be written as

$$C = \omega^k D_{\mathbf{p}} U_G , \qquad G \in SL(2, \mathbb{Z}_p) . \tag{7}$$

In what follows we will be particularly interested in order 3 and order p elements of the Clifford group so we outline some useful facts here. There is a link between the trace of G and the order of G [19]. In prime dimensions, G is of order 3 if and only if $\text{Tr}(G) = -1$. Similarly, G is of order p if $\text{Tr}(G) = 2$, unless G is the identity matrix. Recall we have fixed the phase in Eq. (5) so that U_G has the same order as G.

Clifford unitaries of order 3 have degenerate spectra. There are $p^3(p+1)$ order 3 Clifford elements when $p = 1 \mod 3$ and $p^3(p-1)$ when $p = 2 \mod 3$ [19, 18]. They are called Zauner unitaries, after Zauner who conjectured their relevance to the SIC problem. Later we will confirm the number of Zauner unitaries in the former case using a simple counting argument involving hyperbolic Möbius transformations on the projective line with $p+1$ elements. It is also useful to note that in dimensions $p = 1 \mod 3$ there exists an $H \in SL(2, \mathbb{Z}_p)$ such that HGH^{-1} is diagonal for all G of order 3 [19].

Clifford unitaries of order p sometimes have degenerate spectra. We are interested in those with non-degenerate spectra. The Clifford group contains exactly $p(p+1)(p-1)$ cyclic subgroups of such elements [14]. They relate to the Alltop MUBs, introduced in the next section.

Beyond the Clifford group—where we must venture to perform universal quantum computation—one may add further operators from the Clifford hierarchy [12]. The whole hierarchy can be defined recursively. A unitary U belongs to the kth level of the Clifford hierarchy, if it does not belong to a lower level and for all elements $D_{\mathbf{p}}$ of the Weyl-Heisenberg group, we have that $U D_{\mathbf{p}} U^\dagger$ is an element of the $(k-1)^{\text{th}}$ level of the Clifford hierarchy. The third level of this hierarchy consists of operators that take operators in the Weyl-Heisenberg group to operators in the Clifford group under conjugation. Since the Weyl-Heisenberg operators are of order p and have a non-degenerate spectrum the targets must be operators of order p that cannot be written as

5

Weyl-Heisenberg translates. The third level of the Clifford hierarchy is not a group in itself and includes all operators of the form

$$U = C_1 M^x C_2 \ , \tag{8}$$

where C_1, C_2 are any Clifford unitaries, $x \in \{1, 2, \ldots, p-1\}$ and M is given by

$$M = \sum_r \omega^{r^3} |r\rangle\langle r| \ . \tag{9}$$

The M stands for "magic" [9, 10]. One finds

$$M D_{\mathbf{p}} M^{-1} = \omega^{-\frac{p_1^3}{2}} D_{\mathbf{q}} U_G \ , \tag{10}$$

where

$$\mathbf{q} = \begin{pmatrix} p_1 \\ p_2 + 3p_1^2 \end{pmatrix} \ , \qquad G = \begin{pmatrix} 1 & 0 \\ 6p_1 & 1 \end{pmatrix} \ . \tag{11}$$

The Clifford operation in Eq. (10) is of order p, and its spectrum is non-degenerate. There are altogether $p(p-1)(p^2-1)$ such Clifford group elements and they lie in $p(p+1)(p-1)$ cyclic subgroups [14]. This entire conjugacy class can be obtained by repeatedly conjugating D_p with M and with suitable symplectic group elements.

It is worth noting that the set of all diagonal unitaries up to the third level of the hierarchy does form a group, generated by a displacement operator, an order p symplectic unitary, and M. So the group is $Z_p \times Z_p \times Z_p$. We assume that $p > 3$, but analogues exist also for $p = 3$, and for $p = 2$ where the analogue of M is known as the pi-over-eight gate. Then the analogous abelian subgroups are $Z_3 \times Z_9$ and Z_8, respectively [10].

3   Mutually unbiased bases

We now introduce a complete set of $p + 1$ mutually unbiased bases (MUB), including the computational basis. The vectors in this MUB are collectively known as stabilizer states. The computational basis will be denoted $|I_a^{(0)}\rangle$ where $a \in \{0, 1, \ldots, p-1\}$ labels the vectors and I stands for Ivanović [3]. One gets the rest of the MUB by adding p bases obtained by acting with the

generators of the symplectic group, defined in Eq. (4). Thus, with integers $z \in \{0, 1, \ldots, p - 1\}$,

$$|I_a^{(z)}\rangle = (U_T)^z |I_a^{(0)}\rangle \, , \qquad |I_a^{(\infty)}\rangle = U_F |I_a^{(0)}\rangle \, . \qquad (12)$$

One can check that each of these bases is an eigenbasis of a maximally abelian subgroup of the Weyl-Heisenberg group, which is why they are mutually unbiased [4]. The MUB, or equivalently their labelling set $z \in \{0, 1, \ldots, p - 1, \infty\}$, forms a finite projective line on which the symplectic group acts via Möbius transformations,

$$G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \, , \qquad z \to \frac{\alpha z + \beta}{\gamma z + \delta} \, . \qquad (13)$$

The Weyl-Heisenberg group acts as the identity on this projective line; it permutes vectors within a basis. These Möbius transformations are in many respects analogous to projective transformations of the real projective line. In particular they come in three types: hyperbolic with two fixed points, parabolic with one, and elliptic with no fixed point. A hyperbolic Möbius transformation comes from a matrix G that can be diagonalized by means of conjugation [19]. Order 3 operators give hyperbolic Möbius transformations if and only if $p = 3k + 1$.

We can then count the number of order 3 symplectic unitaries by counting the possible ways of choosing pairs of fixed points. The first fixed point can be any basis in the MUB, for which we have $p + 1$ choices. The second fixed point is a second basis, different to the first, for which we have p choices. Avoiding double counting, this gives $p(p+1)/2$ possible fixed points. As the symplectic unitaries are order 3, U_G^2 has the same fixed points as U_G and so overall we find $p(p+1)$ symplectic unitaries of order 3, as expected. Figure 1 shows a projective line for $p = 7$ where each dot corresponds to a basis in the MUB.
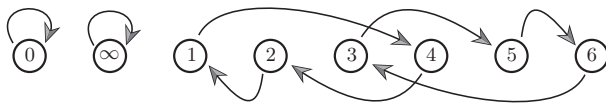

Figure 1: A Möbius transformation of order 3 acting on a projective line with $7 + 1$ elements.

Other MUBs are obtained by acting with operators from the third level of the Clifford hierarchy, such as

$$|A_a^{(z,x)}\rangle = M^x|I_a^{(z)}\rangle\,, \qquad x \in \{1,\ldots,p-1\}\,, \qquad z \in \{0,1,\ldots,p-1,\infty\}\,, \quad (14)$$

where A is for Alltop [13]. (The acronym MUBs is used for multiple complete sets of mutually unbiased bases.) Note that

$$|A_a^{(0,x)}\rangle \sim |I_a^{(0)}\rangle\,, \tag{15}$$

that is to say these two bases are equal up to irrelevant phases. Other Alltop MUBs are obtained by conjugating M with elements of the Clifford group. To avoid burdening our notation too much we give only one example explicitly:

$$|A_a'^{(z,x)}\rangle = U_F M^x U_F^{-1}|I_a^{(z)}\rangle\,, \qquad |A_a'^{(\infty,x)}\rangle \sim |I_a^{(\infty)}\rangle\,. \tag{16}$$

This particular Alltop MUB appears in section 6, where we show that some of the vectors in the MUB are real. Figure 2 shows Alltop vectors generated by M and $U_F M^x U_F^{-1}$ acting on two vectors in the Ivanović MUB.
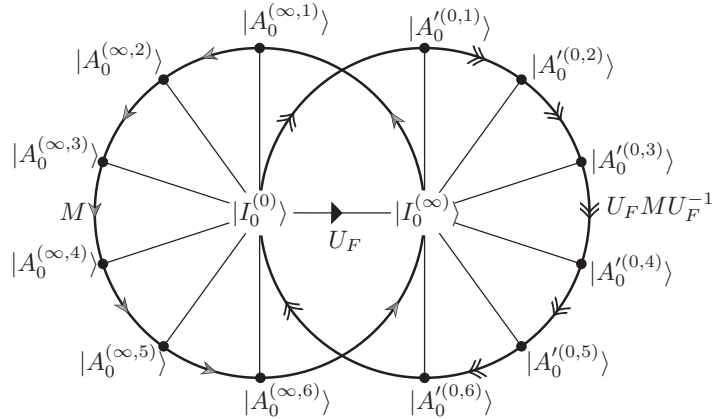

Figure 2: Alltop vectors created by the magical operator from the two fixed vectors in the Ivanović MUB, for $p = 7$.

Altogether this construction leads to $(p+1)(p-1)$ MUBs, each of which contains one basis from Ivanović's MUB. The $p(p+1)(p-1)$ bases unique to the Alltop MUBs are eigenbases of cyclic subgroups containing order p Clifford unitaries with non-degenerate spectra. We see that the number of

these bases matches the number of such subgroups given in the previous section. We refer to these $p^2(p+1)(p-1)$ vectors as Alltop vectors [14], although they are better known as "magic states" in the context of quantum computation [9, 10].

Eq. (14) reveals that the unitary equivalence between Ivanović and Alltop MUB constructions [27] is actually due to a unitary from the third level of the Clifford hierarchy. In addition, Eq. (14) will prove to be a key relationship for establishing that Ivanović and Alltop vectors lie in the same Zauner subspace U_G. Specifically, if $U_G|I_a^{(z)}\rangle = |I_a^{(z)}\rangle$ and U_G and M commute then

$$U_G|A_a^{(z,x)}\rangle = U_G M^x |I_a^{(z)}\rangle = M^x U_G |I_a^{(z)}\rangle = |A_a^{(z,x)}\rangle \ . \tag{17}$$

4 Order 3 symmetries within the Clifford hierarchy

In the previous section we ended by highlighting the importance of symplectic unitaries U_G that commute with the magic unitary M. A simple calculation verifies that

$$MU_G = U_G M \quad \Leftrightarrow \quad G = \begin{pmatrix} \alpha & 0 \\ \gamma & \alpha^2 \end{pmatrix} \quad \text{where} \quad \alpha^3 = 1 \bmod p \ . \tag{18}$$

To enumerate the number of commuting operators we must therefore find the number of integer solutions to the equation $\alpha^3 = 1$ modulo p. The solution $\alpha = 1$ always exists, and the resulting operators are of order p. It is a well known number theoretical fact that two additional solutions exist if and only if $p = 1$ modulo 3. The corresponding group elements are of order 3. Therefore order 3 symmetries have a special status in the hierarchy if and only if $p = 3k + 1$ for some k.

One way of seeing why this case is singled out is to ask for cubic residues: integers x of the form $x = y^3$ modulo p for some integer y. If the dimension is $p = 3k + 2$, then the set of cubic residues equals the whole field $\mathbb{Z}_p$. We can see this by setting $y = x^{2k+1}$, which gives

$$y^3 = \left(x^{2k+1}\right)^3 = x^{6k+3} = x^{3k+2}x^{3k+1} = x^p x^{p-1} = x. \tag{19}$$

The last step uses Fermat's Little Theorem, which states that $x^{p-1} = 1$ modulo p whenever x and p are relatively prime. So every integer y has a distinct cubic residue $x = y^3$ and thus the solution to $\alpha^3 = 1$ is unique.

If the dimension is $p = 3k + 1$ on the other hand, we see that

$$(x^3)^k = (x^3)^{\frac{p-1}{3}} = x^{p-1} = 1 \ . \tag{20}$$

In this case, the cubic residues form a subgroup of order k of the multiplicative group of integers modulo p, dividing it into 3 cosets. This fine structure will be important to us as we proceed.

When $p = 3k + 1$, each order 3 Zauner unitary has an eigenspace of dimension $k + 1$, corresponding to the eigenvalue 1 once its overall phase has been suitably chosen [16]. It is believed that each such Zauner subspace contains a SIC vector (and it is known to be so for $p = 7, 13, 19$ [19, 28] and for $p = 31, 37, 43$ [29]).

It is worth mentioning that a symplectic group element of the form in Eq. (18) is represented by a monomial unitary matrix—see Eq. (5). This simplifies the description of the corresponding Zauner subspaces, and it also simplifies the search for SIC vectors (in these dimensions) [19].

5 Order 3 symmetry of Alltop vectors

We will now show that every Alltop vector is invariant under an order 3 element of the Clifford group, provided the dimension is $p = 3k + 1$. We will focus on a particular such Zauner unitary, because all Zauner unitaries can be obtained from it by conjugating with symplectic unitaries and performing Weyl-Heisenberg translates [30]. We already know that in these dimensions any order 3 symplectic unitary lies in the same conjugacy class as a unitary that corresponds to a diagonal element of $SL(2, \mathbb{Z}_p)$. Without loss of generality we therefore choose as our representative Zauner unitary

$$\mathcal{Z} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^2 \end{pmatrix} \ , \qquad \alpha^3 = 1 \ , \qquad \alpha \neq 1 \ . \tag{21}$$

On the finite projective line of MUB it has fixed points at $z = 0, \infty$. From Eq. (4) we know that the symplectic element F interchanges these fixed points. We check that

10

$$M^{-1}U_{\mathcal{Z}}M = U_{\mathcal{Z}} \ , \qquad U_F^{-1}U_{\mathcal{Z}}U_F = U_{\mathcal{Z}}^2 \ . \tag{22}$$

The first expression is a direct consequence of Eq. (18). Then we observe (again using the explicit representation) that

$$U_{\mathcal{Z}}|I_0^{(0)}\rangle = |I_0^{(0)}\rangle \ , \qquad U_{\mathcal{Z}}|I_0^{(\infty)}\rangle = |I_0^{(\infty)}\rangle \ . \tag{23}$$

The first vector in these two bases, but no other standard MUB vector, is left invariant. Using Eq. (14) it immediately follows that

$$U_{\mathcal{Z}}|A_0^{(\infty,x)}\rangle = |A_0^{(\infty,x)}\rangle \ . \tag{24}$$

Similarly, Eq. (16) leads, after a minor calculation, to

$$U_{\mathcal{Z}}|A_0'^{(0,x)}\rangle = |A_0'^{(0,x)}\rangle \ . \tag{25}$$

The conclusion is that the Zauner subspace contains 2 standard and $2(p-1)$ Alltop vectors. The fact that the Alltop vectors have this extra invariance certainly singles out order 3 operators (in dimensions $p = 3k + 1$) for special attention.

In the other direction, each Ivanović MUB vector is invariant under exactly p^2 Zauner unitaries, since there are p choices for the second fixed point on the projective line, which fixes the symplectic part of the unitary, and then p choices for the Weyl-Heisenberg part of the unitary as each basis vector is invariant under a cyclic subgroup of order p.

Putting everything together, there are $p(p + 1)$ Ivanović MUB vectors, each one of which belongs to p^2 Zauner subspaces, and $(p + 1)p^3/2$ Zauner subspaces each containing 2 Ivanović MUB vectors. This means that the Ivanović MUB constitutes what is known as a configuration of vectors and $(k + 1)$-dimensional subspaces.

In the language of projective geometry, a collection of m points and n lines forms a configuration if each line contains π points and each point has γ lines passing through it. This leads to the condition $m\gamma = n\pi$, fulfilled by all configurations [15]. This is expressed by the notation

$$\left(m_{|\gamma}, n_{|\pi}\right) . \tag{26}$$

For our purposes, a point corresponds to a vector (ray) in Hilbert space and a line corresponds to a subspace. The collection of Ivanović MUB vectors

(stabilizer states) and Zauner subspaces of dimension $k + 1$ can then be written as the configuration

$$\left(p(p+1)_{|p^2}, \frac{(p+1)p^3}{2}_{|2} \right) . \tag{27}$$

More interestingly, the Alltop vectors also form a configuration. We know that each Zauner subspace contains $2(p-1)$ Alltop vectors so now we want to count how many Zauner unitaries leave each Alltop vector invariant. An order 3 Clifford group element leaving an Alltop vector invariant must also leave a special basis in the Ivanović MUB invariant. There are p choices for the symplectic part, but this time there is no freedom in the Weyl-Heisenberg part because no WH operators leave the Alltop vector invariant.

Thus each Alltop vector belongs to p Zauner subspaces, and we obtain the configuration

$$\left((p+1)(p-1)p_{|p}^2, \frac{(p+1)p^3}{2}_{|2(p-1)} \right) . \tag{28}$$

Configurations and their realizations in finite dimensional Hilbert spaces have a distinguished history in mathematics [15, 31], but we are not aware that this particular one has been encountered before.

For $p = 3$, very similar considerations underlie the classical Hesse configuration [24], which consists of 12 Zauner subspaces (orthogonal to 12 MUB vectors) and 9 SIC vectors at their intersections [25]. However, this is a very special case because operators of order 3 are also of order p. Hesse's construction can be generalized to higher prime dimensions in two ways, the present one, and in the direction of the phase point operators introduced by Wootters [32, 33]. The firm connection to SICs is lost in both versions, but the present version does focus on the mysterious order 3 Zauner symmetry in the SIC problem.

From counting arguments it is clear that the Alltop vectors form a single orbit under the Clifford group if $p = 3k + 2$, but three distinct orbits if $p = 3k + 1$, since in this case the number of transformations leaving a particular Alltop vector invariant goes up with a factor of three. To see this explicitly let us ask how we can go between two Alltop vectors belonging to different Weyl-Heisenberg orbits but sitting in the same Zauner subspace. For this purpose we must use a symplectic unitary leaving a particular Ivanović basis, say the one with $z = 0$, invariant. This means that the matrix G must have a zero in the upper right hand corner. One then checks that

12

$$G = \begin{pmatrix} \alpha & 0 \\ \gamma & \delta \end{pmatrix} \quad \Rightarrow \quad U_G M^x = M^{\frac{x}{\alpha^3}} U_G \ , \qquad M^x U_G = U_G M^{x\alpha^3} \ . \quad (29)$$

It follows that

$$U_G |A_a^{(0,x)}\rangle = U_G M^x |I_a^{(0)}\rangle = M^{\frac{x}{\alpha^3}} |I_{a'}^{(0)}\rangle = |A_{a'}^{(0,\frac{x}{\alpha^3})}\rangle \ . \quad (30)$$

In this way we create three multiplets corresponding to the three cosets into which the group of non-zero integers modulo p is divided by the group of cubic residues.

6   Further symmetries of Alltop vectors

For all $p > 3$ the Alltop vectors have a further symmetry, implemented by an anti-unitary operator belonging to the extended Clifford group. The latter is obtained by adjoining the matrix

$$G_K = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (31)$$

to the symplectic group, so that the determinant of the two-by-two matrices are allowed to take the values ± 1 [19]. The matrix G_K is represented in Hilbert space by means of complex conjugation, which we denote by K. An arbitrary anti-unitary operator can be written as UK, where U is unitary and K denotes complex conjugation in a given basis [34]. Vectors invariant under an anti-unitary operator form a real subspace of Hilbert space—although it depends on the choice of basis whether the entries of these vectors are real numbers, or not.

Consider also the unique order 2 element of the symplectic group,

$$A = F^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \Rightarrow \quad G_K A = F^{-1} G_K F \ . \quad (32)$$

The Weyl-Heisenberg translates of A are identical to Wootters' phase point operators [33], provided we choose the positive sign in Eq. (5), and we do so for convenience. The phase for the unitary matrix U_F is chosen so that it becomes identical to the usual Fourier matrix. Each vector in the Ivanović

MUB is invariant under an element of the Clifford group of order two, in particular the vectors $|I_0^{(z)}\rangle$ are invariant under U_A. The vectors $|I_0^{(0)}\rangle$ and $|I_0^{(\infty)}\rangle$ are special in that they are also invariant under complex conjugation.

To see what this implies for the Alltop MUBs we again focus on the magic operator M. It commutes with the anti-unitary operator $U_A K$,

$$M U_A K = U_A K M \ . \tag{33}$$

For the Alltop MUBs that include the computational basis, it follows that

$$U_A K |A_0^{(\infty,x)}\rangle = U_A K M |I_0^{(\infty)}\rangle = M U_A K |I_0^{(\infty)}\rangle = |A_0^{(\infty,x)}\rangle \ . \tag{34}$$

There is another Alltop MUB obtained by conjugating the magic operator with U_F, namely

$$|A_a'^{(z,x)}\rangle = U_F M^x U_F^{-1} |I_a^{(z)}\rangle \ . \tag{35}$$

This MUB includes the Fourier basis and was given earlier in Eq. (16). Using $U_A = U_F^2$ and $K U_F = U_F^3 K$ it is easy to show that

$$K |A_0'^{(0,x)}\rangle = |A_0'^{(0,x)}\rangle \ . \tag{36}$$

These particular Alltop vectors are manifestly real. The conclusion so far is that Alltop vectors lie in real subspaces. Each such real subspace contains $p-1$ distinct Alltop vectors, labelled by x.

If the dimension is $p = 3k+1$ we know that each Zauner subspace contains $2(p-1)$ Alltop vectors. Let us again focus on the representative Zauner operator $U_{\mathcal{Z}}$, which commutes with M, K and $U_A K$. In this case, the $p-1$ Alltop vectors $|A_0^{(\infty,x)}\rangle$ lie in the intersection of the Zauner subspace with the real subspace invariant under $U_A K$, and the $p-1$ Alltop vectors $|A_0'^{(0,x)}\rangle$ in its intersection with the manifestly real subspace.

Thus the conclusion, when the dimension is a prime equal to 1 modulo 3, is that the $2(p-1)$ Alltop vectors in a given Zauner subspace are to be found in equal numbers in its intersections with two real subspaces. For $p = 7$, 19 there also exist SIC vectors in these intersections [19], but this does not seem to happen for any other value of p [35].

14

7 Relationship of Alltop vectors to Quantum Computation

The set of Clifford unitaries and Pauli measurements are collectively known as stabilizer operations and these operations arise naturally in the context of fault-tolerant quantum computing (QC). The most promising proposals for building a large-scale quantum computer use error-correcting codes for which stabilizer operations are provably fault-tolerant (i.e., they do not introduce errors in an uncontrollable way) [2]. The stabilizer operations include all Clifford unitaries, Pauli measurements (with adaptive feedforward), preparation of stabilizer states and tracing out any subsystems. Unfortunately, any circuit using only stabilizer operations (applied to an initial computational-basis input state) is no more powerful than a classical computer, so some additional capability is needed. This fact has motivated the magic state model [6, 7] of QC whereby special resource states—magic states—are used up to implement non-Clifford unitaries. Stabilizer circuits supplemented by a supply of magic states are capable of universal and fault-tolerant quantum computing.

The connection to our work is via the Alltop vectors, which are precisely the magic states in prime dimensions. We have seen that the Alltop vectors are related to the Ivanović MUB by an element at the third level of the Clifford hierarchy. In quantum computing language, this statement becomes that the magic states are related to the stabilizer states by an element at the third level of the Clifford hierarchy. This was first studied for qubits [6, 7] and then extended to higher-dimensional qudit systems [9, 10]. Furthermore, we have seen that up to Clifford unitaries these magic states split into either a single equivalence class (if $p = 2 \bmod 3$) or three equivalence classes (if $p = 1 \bmod 3$).

Clifford inequivalent quantum states vary in their potential as a computational resource in the magic states model, and this can be quantified by magic monotones. Veitch *et. al.* [37] proposed two such measures and here we comment on the relevance of one of them—the *mana* $\mathcal{M}$—to our results. The mana for an n qudit state ρ is easily calculated from

$$\mathcal{M}(\rho) = \ln \left(\sum_{r=1}^{d^2} |W_\rho(r)| \right) \tag{37}$$

where $W_\rho(r)$ denotes the components of the Wigner function [33]. From this

definition follow numerous intuitive properties including

1. For all stabilizer states ρ_{stab}, the mana vanishes $\mathcal{M}(\rho_{\text{stab}}) = 0$;

2. Positivity, for all ρ, $\mathcal{M}(\rho) \geq 0$;

3. Additivity: for all ρ, σ, it follows $\mathcal{M}(\rho \otimes \sigma) = \mathcal{M}(\rho) + \mathcal{M}(\sigma)$;

4. Clifford invariance: for all Clifford C, it holds that $\mathcal{M}(C\rho C^{\dagger}) = \mathcal{M}(\rho)$;

5. Monotonicity: for all trace preserving quantum channels $\mathcal{E}$ composed from stabilizer operations, and for all ρ, we have $\mathcal{M}[\mathcal{E}(\rho)] \leq \mathcal{M}(\rho)$.

These properties make mana especially relevant to quantum computation. Envisage a quantum circuit producing a multi-qudit state σ, and we must simulate this using only stabilizer operations and a supply of a magic states ρ. Combining monotonicity with additivity, we infer that one needs at least $n = \mathcal{M}(\sigma)/\mathcal{M}(\rho)$ copies of ρ. The less mana contained in ρ, the more copies we need for a given computation. This naturally prompts the question "how much mana do the Alltop vectors have?" By Clifford invariance we know that all vectors $\left|A_a^{(z,x)}\right\rangle$ within the same Clifford orbit will have the same mana. However, when $p = 1 \bmod 3$, it becomes possible for different Alltop vectors to carry more or less mana. For instance, when $p = 7$ we can use $x = 1, 2, 3$ as representatives of the three distinct equivalence classes of Alltop vectors, and find

$$\mathcal{M}\left(\left|A_a^{(z,1)}\right\rangle\right) = 0.8148, \tag{38}$$

$$\mathcal{M}\left(\left|A_a^{(z,2)}\right\rangle\right) = 0.8148, \tag{39}$$

$$\mathcal{M}\left(\left|A_a^{(z,3)}\right\rangle\right) = 0.8962. \tag{40}$$

This hints that the vectors with $x = 3$ might be a more powerful resource for quantum computation. One must be cautious about jumping to this conclusion since mana is not the unique magic monotone with the aforementioned properties.

Since we are also interested in SICs, we comment on the mana of SIC vectors. There are two Clifford orbits of SICs in $p = 7$ and we find

$$\mathcal{M}(\psi_{\text{SIC}}^a) = 0.8354, \tag{41}$$

$$\mathcal{M}(\psi_{\text{SIC}}^b) = 0.8116, \tag{42}$$

where ψ_{SIC}^a corresponds to the fiducial $7a$ and ψ_{SIC}^b corresponds to $7b$ in [20]. In $p = 7$, the state with maximal mana has $\mathcal{M} = 0.9022$ [36].

16

8 Conclusions

In the context of quantum computation, the most interesting aspect of our current work is that it identifies an unexpected additional structure for magic states in prime dimensions of the form $p = 1 \bmod 3$—not all magic states are created equal. In dimensions of the form $p = 2 \bmod 3$, every magic state can be converted to an equivalent magic state by means of a Clifford gate, meaning that all these magic states exhibit the same amount of robustness to noise [10] or mana (quantified as a resource [37]). In dimensions $p = 1 \bmod 3$, the partitioning of Alltop vectors into three distinct Clifford orbits means this no longer holds true, and magic states from a particular orbit can be preferable to states from the remaining orbits.

We also aimed to throw a glimmer of light on the SIC existence problem. If the dimension of Hilbert space is a prime number p it seems reasonable to hope for a connection to mutually unbiased bases, which—in their Alltop guise—form another distinguished orbit under the Weyl-Heisenberg group. For $p = 3$ the connection is very firm. A hint that a connection exists for all p is known [22, 23], and prime dimensions do seem to be worth special attention [18]. We observed that the Zauner subspaces—in which the SIC vectors are expected to lie—and the Alltop vectors form a configuration whenever $p = 1 \bmod 3$. In this case at least the order 3 Zauner symmetry plays a special role for Alltop and SIC orbits alike. We believe that this considerably strengthens the case for a connection. The Zauner subspaces are no longer featureless.

Acknowledgements:

References

[1] J. Schwinger: *Quantum Mechanics. Symbolism of Atomic Measurements*, ed. by B.-G. Englert, Springer, Berlin 2001.

[2] D. Gottesman, *Theory of fault-tolerant quantum computation*, Phys. Rev. A **57** (1998) 127.

[3] I. D. Ivanović, *Geometrical description of state determination*, *J. Phys.* **A14** (1981) 3241.

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

[5] D. Gottesman, *The Heisenberg Representation of Quantum Computers*, arXiv:quant-ph/9807006 (1998)

[6] S. Bravyi and A. Kitaev, *Universal quantum computation with ideal Clifford gates and noisy ancillas*, Phys. Rev. **A71** (2005) 022316.

[7] E. Knill, *Quantum Computing with Realistically Noisy Devices*, Nature **434** (2005) 39.

[8] H. Anwar, E. T. Campbell and D. E. Browne, *Qutrit magic state distillation*, New Journal of Physics **14** (2012) 063006.

[9] E. T. Campbell, H. Anwar and D. E. Browne, *Magic state distillation in all prime dimensions using quantum Reed-Muller codes*, Phys. Rev. **X2** (2012) 041021.

[10] M. Howard and J. Vala, *Qudit versions of the qubit "pi-over-eight" gate*, Phys. Rev. **A86** (2012) 022316.

[11] E. T. Campbell, *Enhanced fault-tolerant quantum computing in d-level systems*, arXiv:1406.3055 [quant-ph].

[12] D. Gottesman and I. L. Chuang, *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations*, Nature **402** (1999) 390.

[13] W. O. Alltop, *Complex sequences with low periodic correlations*, IEEE Trans. Inf. Theory **26** (1980) 350.

[14] K. Blanchfield, *Orbits of mutually unbiased bases*, J. Phys. A: Math. Theor. **47** (2014) 135303.

[15] D. Hilbert and S. Cohn-Vossen: *Anschauliche Geometrie*, Springer, Berlin 1932.

[16] G. Zauner: *Quantendesigns. Grundzüge einer nichtkommutativen Designtheorie*, PhD thesis, Univ. Wien 1999. Available in English translation in Int. J. Quant. Inf. **9** (2011) 445.

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

[18] H. Zhu, *SIC-POVMs and Clifford groups in prime dimensions*, J. Phys. **A43** (2010) 305305.

[19] D. M. Appleby, *SIC-POVMs and the extended Clifford group*, J. Math. Phys. **46**, (2005) 052107.

[20] A. J. Scott and M. Grassl, *SIC-POVMs: A new computer study*, J. Math. Phys. **51** (2010) 042203.

[21] D. M. Appleby, C. A. Fuchs and H. Zhu, *Group theoretic, Lie algebraic and Jordan algebraic formulations of the SIC existence problem*, eprint arXiv:1312.0555.

[22] D. M. Appleby, H. B. Dang and C. A. Fuchs, *Symmetric Informationally-Complete quantum states as analogues to orthonormal bases and Minimum Uncertainty States*, Entropy **16** (2014) 1484.

[23] D. M. Appleby, *SIC-POVMs and MUBs: Geometrical relationships in prime dimensions*, in L. Accardi et al (eds.): Proc of the Växjö Conference on Foundations of Probability and Physics - 5, AIP Conf. Proc. **1101**, New York 2009.

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

[25] H. B. Dang, K. Blanchfield, I. Bengtsson and D. M. Appleby, *Linear dependencies in Weyl-Heisenberg orbits*, Quant. Inf. Proc. **12** (2013) 3449.

[26] D. M. Appleby, *Properties of the extended Clifford group with applications to SIC-POVMs and MUBs*, arXiv:0909.5233 [quant-ph] (2009).

[27] C. Godsil and A. Roy, *Equiangular lines, mutually unbiased bases, and spin models*, European Journal of Combinatorics, **30** (2009) 246.

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

[29] D. M. Appleby, private communication (2011).

[30] S. T. Flammia, *On SIC-POVMs in Prime Dimensions*, J. Phys. A: Math. Gen. **39** (2006) 13483.

[31] I. Dolgachev, *Abstract configurations in algebraic geometry*, in Proc. of the Fano Conference, Univ. Torino, Torino 2004.

[32] C. Segre, *Remarques sur les transformations uniformes des courbes elliptiques en elles-mèmes*, Math. Ann. **27** (1886) 296.

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

[34] E. Wigner, *Normal form of antiunitary operators*, J. Math. Phys. **1** (1960) 409.

[35] M. Khaterinejad, *On Weyl-Heisenberg orbits of equiangular lines*, J. Algebra. Comb. **28** (2008) 333.

[36] G. N. M. Tabia and D. M. Appleby, private communication (2014).

[37] V. Veitch, S. A. H. Mousavian, D. Gottesman and J. Emerson, *The Resource Theory of Stabilizer Computation*, New J. Phys. **16** (2014) 013009.