PROPERTIES OF THE EXTENDED CLIFFORD GROUP WITH APPLICATIONS TO SIC-POVMS AND MUBS.

D M APPLEBY

Perimeter Institute for Theoretical Physics
Waterloo, Ontario N2L 2Y5, Canada

(E-mail: mappleby@perimeterinstitute.ca)

We consider a version of the extended Clifford Group which is defined in terms of a finite Galois field in odd prime power dimension. We show that Neuhauser's result, that with the appropriate choice of phases the standard (or metaplectic) representation of the discrete symplectic group is faithful (as opposed to merely projective), also holds for the anti-unitary operators of the extended group. We also improve on Neuhauser's result by giving explicit formulae which enable one easily to calculate the (anti-)unitary corresponding to an arbitrary (anti-)symplectic matrix. We then go on to find the eigenvalues of an arbitrary (anti-)symplectic matrix. The fact that in prime power dimension the matrix elements belong to a field means that this can be done using the same techniques which are used to find the eigenvalues of a matrix defined over the reals—including the use of an extension field (the analogue of the complex numbers) when the eigenvalues are not in the base field. With the eigenvalues of the (anti-)symplectic matrix in hand it is straightforward to find the eigenvalues, the order and all roots of the corresponding (anti-)unitary. We then give an application of these results to SIC-POVMs (symmetric informationally complete positive operator valued measures). We show that in prime dimension our results can be used to find a natural basis for the eigenspace of the Zauner unitary in which SIC-fiducials are expected to lie. We go on to use the extension field to construct a parameterization of the displacement operators analagous to the one commonly employed in quantum optics, using the complex eigenvalues of the annihilation operator. Finally, we apply our results to the MUB cycling problem. Wootters and Sussman have shown that in every even prime power dimension there is a single Clifford unitary which cycles through a full set of MUBs (mutually unbiassed bases). We show that in odd prime power dimension d, although there is no Clifford unitary, there is a Clifford anti-unitary which cycles through the full set of Wootters-Fields MUBs if $d = 3 \pmod 4$. Also, irrespective of whether $d = 1$ or $3 \pmod 4$, the Wootters-Fields MUBs split into two groups of $(d+1)/2$ bases in such a way that there is a single Clifford unitary which cycles through each group separately.

1. INTRODUCTION

Since its original introduction into the field of quantum information the Clifford group [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30] has found numerous applications. Our own interest in the group, and the extended Clifford Group [12, 28] of which it is a subgroup, is due to their role in the theory of mutually unbiassed bases (MUBs) [11, 18, 19, 21, 25, 26, 28, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63] and symmetric, informationally complete positive operator valued measures (SIC-POVMs) [12, 17, 23, 41, 45, 50, 51, 55, 59, 60, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80]. However, the results we derive along the way may be of wider interest.

We should remark at the outset that it is possible to identify at least three different (though closely related) mathematical constructs which commonly go by the name "Clifford group". We will clarify the precise sense in which we are using the term in Section 2 (see paragraph following Eq. (28)). For now we will confine ourselves to saying that we are concerned with a version of the Clifford group which is defined over a finite field [82], and which therefore only exists in prime power dimension. There are some significant complications when the dimension is a power of 2, so in this paper we confine ourselves to the case of odd prime power dimension. We hope to treat the even prime power case in a subsequent paper.

In the first part of the paper (sections 2 to 5) we prove a number of general results concerning the Clifford and extended Clifford groups. In the second part we apply these results to a problem which arises in the theory of SIC-POVMs and to the MUB cycling problem. We also show how they can be used to construct an alternative parameterization of the displacement operators. In a subsequent paper we will use them to complete the proof that the minimum uncertainty states introduced by Wootters and Sussman [25, 26] and Appleby, Dang and Fuchs [77] exist in every prime power dimension.

The Clifford group is built out of two kinds of operator: displacement operators $D_{\mathbf{u}}$, labelled by vectors of the form

$$\mathbf{u} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \tag{1}$$

with components in the finite field $\mathbb{F}_d$ (d being the Hilbert space dimension), and symplectic unitaries U_F, labelled by 2×2 matrices of the form

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{2}$$

with elements in $\mathbb{F}_d$ and determinant $= 1$. The set of all such matrices constitutes the (discrete) symplectic group, $\mathrm{SL}(2, \mathbb{F}_d)$. The symplectic unitaries permute the displacement operators according to the prescription

$$U_F D_{\mathbf{u}} U_F^{\dagger} = D_{F\mathbf{u}} \tag{3}$$

Explicit expressions for the operators $D_{\mathbf{u}}$ and U_F will be given below.

The extended Clifford group is built out of the above operators together with anti-symplectic anti-unitaries U_F, for which the matrix F has determinant $= -1$. We refer to the set of all 2×2 matrices with either sign of the determinant as the extended symplectic group $\mathrm{ESL}(2, \mathbb{F}_d)$.

After reviewing what is already known on this subject in Section 2 we begin our analysis in Section 3 by showing that the phases of the operators U_F can be chosen in such a way that the map $F \to U_F$ (the metaplectic representation [4, 22]) becomes a faithful representation of the group $\mathrm{ESL}(2, \mathbb{F}_d)$, as opposed to one that is merely projective. In other words

$$U_{F_1} U_{F_2} = U_{F_1 F_2} \tag{4}$$

for all F_1, F_2. The fact that this is possible for the group $\mathrm{SL}(2, \mathbb{F}_d)$ was shown by Neuhauser [4]. We establish that the result extends to $\mathrm{ESL}(2, \mathbb{F}_d)$. We also improve on Neuhauser's result by giving explicit formulae which enable one easily to calculate U_F for any given matrix F. In fact we give two different sets of formulae for, in addition to giving explicit expressions for the matrix elements, we show (in Section 4) that U_F can be simply expressed as a linear combination of displacement operators.

We next (Section 5) consider the problem of finding the order of an arbitrary symplectic/anti-symplectic operator U_F (*i.e.* the smallest positive integer m such that $U_F^m = 1$), its eigenvalues and eigenspaces, and its roots. To solve this problem we make essential use of the fact that $\mathbb{F}_d$ is a field. This means that we can use exactly the same techniques to diagonalize a matrix

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{5}$$

with elements $\in \mathbb{F}_d$ that we would if its elements were real numbers. In particular we can use the trick of going to an extension field. If it should happen that the characteristic equation of a matrix over the reals has no real solutions, then we simply embed the reals in the field of complex numbers. Similarly here: if the matrix F has no eigenvalues in $\mathbb{F}_d$ we can embed $\mathbb{F}_d$ in the extension field $\mathbb{F}_{d^2}$. Once one knows the eigenvalues, finding the order is a comparatively simple matter. We give explicit formulae which enable one easily to calculate the order of an arbitrary matrix $F \in \mathrm{ESL}(2, \mathbb{F}_d)$. With these formulae in hand it is straightforward to calculate the order, eigenspaces and eigenvalues, and roots of the corresponding unitary/anti-unitary U_F.

In Section 6 we apply the methods developed in the previous sections to a problem which arises in theory of SIC-POVMs. Scott and Grassl's [80] recent exhaustive numerical investigation encourages the speculation that, in all dimensions, every Weyl-Heisenberg covariant SIC-fiducial is an eigenvector of a canonical order 3 Clifford unitary [12]. Generally speaking this unitary belongs to a different version of the Clifford group than the one considered here. However, if the dimension is prime (as opposed to a power > 1 of a prime) the two versions are the same, and the results obtained in this paper become applicable. We show how they can be used to find a natural basis for the eigenspace of the order 3 symplectic unitary in which SIC-fiducials are expected to lie.

In Section 7 we describe an alternative labelling of the displacement operators. In quantum optics it is usual to parameterise the (continuous variable) displacement operators with the complex variable

$$\alpha = \frac{1}{\sqrt{2}}(q + ip) \tag{6}$$

(where q, p are the quadratures). A similar construction can be carried through in the discrete case, using the extension field $\mathbb{F}_{d^2}$ instead of $\mathbb{C}$. Taking the discrete logarithm we obtain an integer labelling of the displacement operators, which leads to a natural way of representing $\mathrm{ESL}(2, \mathbb{F}_d)$ as a group of permutation matrices. This result is needed in Section 10, but it may be of some independent interest.

Finally, in Sections 8 to 10 we consider the MUB-cycling problem. Wootters and Sussman [25, 26] have shown that in every dimension equal to a power of 2 there exists a single Clifford unitary which cycles through a full set of MUBs. We investigate the situation in odd prime power dimension. We show that in this case there is no single Clifford unitary which cycles through the full set of Wootters-Fields MUBs [33] (at least for the version of the Clifford group considered here—see below). However, if $d = 3 \pmod 4$ there is a single *anti*-Clifford *anti*-unitary which cycles through them. Furthermore, it is possible, for all odd prime power d, to split the Wootters-Fields MUBs into two groups of $(d+1)/2$ bases each in such a way that there is a single Clifford unitary which cycles through each group separately (we say that a unitary with this property is half-cycling). This leads to a natural labelling scheme for the MUBs, in which a cycling anti-unitary (when it exists) increases the integer index by 1 and a half-cycling unitary increases it by 2.

Wootters and Sussman [25] used the existence of cycling unitaries in even prime power dimension to prove the existence of minimum uncertainty states in all such dimensions. Sussman [26] subsequently extended the proof to an infinite subset of the prime power dimensions $= 3 \pmod 4$. In a subsequent paper we will use the results obtained in Sections 8 to 10 of this paper to complete the proof, and to show that minimum uncertainty states exist in all prime power dimensions, without exception.

2. Preliminaries

We begin by reviewing some relevant definitions and known facts concerning Galoisian variants of the Clifford and extended Clifford groups [4, 5, 6, 9, 10, 11, 17, 19, 20, 22, 24, 25, 26, 28, 33, 38, 39, 42, 44, 47, 48, 50, 54, 56]. This will also allow us to clarify the relation between the version of the Clifford group considered in this paper and definitions used by other authors.

Let us begin by defining the Galoisian variant of the Weyl-Heisenberg group (or generalized Pauli group). The ordinary Weyl-Heisenberg group is defined by choosing an orthonormal basis $|0\rangle, |1\rangle, \ldots, |d-1\rangle$ in d-dimensional Hilbert space and then defining operators X and Z by

$$X|x\rangle = |x+1\rangle \tag{7}$$

$$Z|x\rangle = \omega^x |x\rangle \tag{8}$$

where $\omega = e^{\frac{2\pi i}{d}}$ and addition of indices is mod d. If d is odd the Weyl-Heisenberg group is the group generated by these operators (in even dimension there is a slight complication—see, for example, ref. [12]). In dimension $d = p^n$, where p is a prime number and n is a positive integer, the Galoisian variant of the Weyl-Heisenberg group is defined similarly except that instead of labelling the orthonormal basis by the integers mod d one labels them by the elements of the finite field $\mathbb{F}_d$ (for a summary account of the aspects of the theory of finite fields which are relevant here see, for example, Vourdas [20], Pittenger and Rubin [38] or Klimov *et al* [54]; for a more comprehensive treatment see, for example, Lidl and Niederreiter [82]).

One then defines, for all $x, u \in \mathbb{F}_d$,

$$X_u |x\rangle = |x + u\rangle \tag{9}$$

$$Z_u |x\rangle = \omega^{\mathrm{tr}(xu)} |x\rangle \tag{10}$$

where $\omega = e^{\frac{2\pi i}{p}}$ (observe that ω is now a pth root of unity, not a dth root of unity as in the case of the ordinary variant), and where $\mathrm{tr}\colon \mathbb{F}_d \to \mathbb{Z}_p$ is the field theoretic trace defined by

$$\mathrm{tr}(x) = \sum_{r=0}^{n-1} x^{(p^r)} \tag{11}$$

(making the natural identification of $\mathbb{Z}_p$, the integers modulo p, with the set $\{z \in \mathbb{F}_d \colon z^p = z\}$). Notice that if $n > 1$ we cannot write $X_u = X^u$, $Z_u = Z^u$ because it does, in general, make no sense to raise a Hilbert space operator to the power of an element of a finite field. However if $n = 1$ we can identify $\mathbb{F}_d$ with $\mathbb{Z}_p$, which means we can make these replacements, and the Galoisian variant of the Weyl-Heisenberg group becomes identical with the ordinary variant.

Next, for each vector $\mathbf{u} = (u_1, u_2) \in \mathbb{F}_d^2$, define the displacement operator

$$D_{\mathbf{u}} = \tau^{\mathrm{tr}(u_1 u_2)} X_{u_1} Z_{u_2} \tag{12}$$

where $\tau = \omega^{\frac{p+1}{2}}$. Note that $\tau^2 = \omega$ and that τ, like ω, is a pth root of unity. We have, as an immediate consequence of this definition,

$$D_{\mathbf{u}}^\dagger = D_{-\mathbf{u}} \tag{13}$$

and

$$D_{\mathbf{u}} D_{\mathbf{v}} = \tau^{\langle \mathbf{u}, \mathbf{v} \rangle} D_{\mathbf{u}+\mathbf{v}} \tag{14}$$

where $\langle \mathbf{u}, \mathbf{v} \rangle$ is the symplectic form

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathrm{tr}(u_2 v_1 - u_1 v_2) \tag{15}$$

It follows that

$$(D_{\mathbf{u}})^k = D_{k\mathbf{r}} \tag{16}$$

for every integer k and all $\mathbf{u} \in \mathbb{F}_d$. In particular

$$(D_{\mathbf{u}})^p = 1 \tag{17}$$

So the displacement operators are all order p (apart from $D_{\mathbf{0}}$).

It can be seen from the above that the set of operators $\{\omega^m D_{\mathbf{u}} \colon \mathbf{u} \in \mathbb{F}_d, \, m \in \mathbb{Z}_p\}$ constitutes a group, which is what we are calling the Galoisian variant of the Weyl-Heisenberg group, and which we will denote $\mathcal{W}_d$.

Many authors define $\mathcal{W}_d$ in a way that may look, on the face of it, rather different, as a tensor product of n copies of the ordinary variant of the Weyl-Heisenberg group in dimension p (the "many-particle" definition, in Gross's [17, 22, 27, 81] terminology). To see that this definition is in fact equivalent to ours let e_r be any basis for the field $\mathbb{F}_d$, and let $\bar{e}_r$ be the dual basis. So

$$\mathrm{tr}(e_r \bar{e}_s) = \delta_{r,s} \tag{18}$$

for all r, s. For arbitrary $x \in \mathbb{F}_d$ let $x_r = \mathrm{tr}(x\bar{e}_r)$ (respectively $\bar{x}_r = \mathrm{tr}(xe_r)$) be its expansion coefficients relative to the basis e_r (respectively $\bar{e}_r$). So

$$x = \sum_{r=1}^{n} x_r e_r = \sum_{r=1}^{n} \bar{x}_r \bar{e}_r \tag{19}$$

Let $\mathcal{H}_p$ (respectively $\mathcal{H}_d$) be p-dimensional (respectively d-dimensional) Hilbert space, and let $|0\rangle, \dots, |p-1\rangle$ be the standard basis for $\mathcal{H}_p$. Let $D_{\mathbf{u}}^p$ be the ordinary Weyl-Heisenberg displacement operators in dimension p. So

$$D_{\mathbf{u}}^p|k\rangle = \tau^{u_1 u_2 + 2k u_2}|k + u_1\rangle \tag{20}$$

Finally, let $S\colon \mathcal{H}_d \to \mathcal{H}_p \otimes \dots \mathcal{H}_p$ be the linear isomorphism whose action on the basis states is

$$S|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle \tag{21}$$

Then

$$D_{\mathbf{u}} = D_{(u_1,u_2)} = S^{-1}\left(D_{(u_{11},\bar{u}_{21})}^p \otimes \cdots \otimes D_{(u_{1n},\bar{u}_{2n})}^p\right) S \tag{22}$$

for all $\mathbf{u}$ (where $u_{1r} = \mathrm{tr}(u_1\bar{e}_r)$, $\bar{u}_{2r} = \mathrm{tr}(u_2 e_r)$). This defines an isomorphism of the groups $\mathcal{W}_p \otimes \cdots \otimes \mathcal{W}_p$ and $\mathcal{W}_d$. Note, however, that it is not a *natural* isomorphism (because there are many pairs of dual bases for the field $\mathbb{F}_d$).

These definitions (the one we gave earlier, and the one which consists in identifying $\mathcal{W}_d$ with the tensor product $\mathcal{W}_p \otimes \cdots \otimes \mathcal{W}_p$) both have their advantages. The tensor product definition is, perhaps, the more natural of the two in a situation such as occurs when one has a register consisting of n different p-dits. In a situation like that the tensor product structure reflects the actual physics. Also the tensor product definition may be found attractive because it makes no reference to the mathematics of Galois fields, which is unfamiliar to many physicists. However, those advantages partly disappear if one is interested in a single qudit which doesn't naturally split into a product of n different p-dits. In that case the imposition of an (arbitrary) tensor product structure introduces a needless complication. Moreover, even in a situation where the system of interest does in fact consist of n distinct p-dimensional subsystems one might want to make use of the properties of Galois fields. In a case like that, given that one is going to have to introduce them eventually, it would seem to make sense to introduce Galois fields right at the outset, in the definition itself. In this paper we are going to make very heavy use of Galois fields. We consequently prefer our definition.

Let us now turn to the definition of the Galoisian variant of the Clifford group. Here again we have a choice between two alternative definitions. However, whereas in the case of $\mathcal{W}_d$ it is essentially a matter of taste which definition one prefers, here the choice is substantive in that the groups defined are non-isomorphic. Let us begin with what we will call the unrestricted (Galoisian) Clifford group, $\mathcal{C}_d$. This is the set of unitaries U which reshuffle and re-phase the displacement operators, according to the prescription

$$U D_{\mathbf{u}} U^\dagger = e^{ig(\mathbf{u})} D_{f(\mathbf{u})} \tag{23}$$

for all $\mathbf{u}$ and suitable U-dependent functions f, g. Since $D_{\mathbf{u}}^p = 1$ for all $\mathbf{u}$ the phase $e^{ig(\mathbf{p})}$ must be a pth root of unity. So we must in fact have

$$U D_{\mathbf{u}} U^\dagger = \omega^{h(\mathbf{u})} D_{f(\mathbf{u})} \tag{24}$$

for some function h taking values in $\mathbb{Z}_p$. In other words $\mathcal{C}_d$ is the normalizer of $\mathcal{W}_d$ (*i.e.* it is the set of unitaries U such that $U\mathcal{W}_d U^\dagger = \mathcal{W}_d$).

It follows from Eq. (14) that, for any such U, we must have

$$\tau^{2h(\mathbf{u})+2h(\mathbf{v})+\langle f(\mathbf{u}),f(\mathbf{v})\rangle} D_{f(\mathbf{u})+f(\mathbf{v})} = U D_{\mathbf{u}} D_{\mathbf{v}} U^\dagger = \tau^{2h(\mathbf{u}+\mathbf{v})+\langle \mathbf{u},\mathbf{v}\rangle} D_{f(\mathbf{u}+\mathbf{v})} \quad (25)$$

for all $\mathbf{u}, \mathbf{v}$. So the function f must have the property

$$f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) \quad (26)$$

In particular

$$f(m\mathbf{u}) = f(\mathbf{u} + \cdots + \mathbf{u}) = mf(\mathbf{u}) \quad (27)$$

for all $m \in \mathbb{Z}_p$. We will refer to a function with this property as p-linear.

We define the restricted (Galoisian) Clifford group $\mathcal{C}_d^{\mathrm{r}}$ to be the subgroup of $\mathcal{C}_d$ comprising those unitaries which satisfy the additional requirement that f be, not merely p-linear, but d-linear in the sense

$$f(x\mathbf{u}) = xf(\mathbf{u}) \quad (28)$$

for all $x \in \mathbb{F}_d$.

Some authors (for example Cormick *et al* [21]) use the term "Clifford Group" to mean $\mathcal{C}_d$; others (for example Vourdas [24]) use it to mean $\mathcal{C}_d^{\mathrm{r}}$. Gross [17, 22, 27, 81] has proposed to resolve the ambiguity by referring to $\mathcal{C}_d$ as the "many-particle" Clifford group, and to $\mathcal{C}_d^{\mathrm{r}}$ as the "single-particle" Clifford group. We have not adopted Gross's terminology ourselves because it seems to us that the mathematical distinction between the groups $\mathcal{C}_d$ and $\mathcal{C}_d^{\mathrm{r}}$ has nothing specially to do with the distinction between composite and non-composite physical systems. Suppose we have a non-composite physical system, and suppose we adopt the "single-particle" definition (in Gross's terminology) of $\mathcal{W}_d$, as represented by Eqs. (9) and (10). Then we will still be faced with the fact that the normalizer of $\mathcal{W}_d$ is $\mathcal{C}_d$, not $\mathcal{C}_d^{\mathrm{r}}$. So $\mathcal{C}_d$ is no less relevant to single-particle systems than it is to many-particle ones. The reason is that the distinction between p-linearity and d-linearity does not depend on the assumption of a tensor product structure. It therefore seems to us that our terminology, referring to $\mathcal{C}_d$ as the unrestricted group and to $\mathcal{C}_d^{\mathrm{r}}$ as the restricted group, is more appropriate.

In this paper we will focus on the restricted group, $\mathcal{C}_d^{\mathrm{r}}$. This is not because we consider $\mathcal{C}_d^{\mathrm{r}}$ to be of greater physical and/or mathematical importance than $\mathcal{C}_d$. Nor is it because we are more interested in single-particle systems than many-particle ones. It is just that the d-linear transformations of $\mathcal{C}_d^{\mathrm{r}}$ have a number of nice properties which make them worthy of separate investigation. In particular, they have all the properties needed to prove the existence of minimum uncertainty states in every odd prime power dimension (which was the problem that originally motivated this research). We have therefore chosen to focus on $\mathcal{C}_d^{\mathrm{r}}$ in this paper, and to defer a discussion of $\mathcal{C}_d$ to what we hope will be another, subsequent paper.

If it is assumed that f is d-linear Eq. (25) implies

(a) The function f is of the form

$$f(\mathbf{u}) = F\mathbf{u} \quad (29)$$

where $F \in \mathrm{SL}(2, \mathbb{F}_d)$—*i.e.* is a 2×2 matrix

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad (30)$$

with entries in $\mathbb{F}_d$ and such that $\det F = 1$.

(b) The function g is of the form

$$g(\mathbf{u}) = \langle \boldsymbol{\chi}, \mathbf{u} \rangle \tag{31}$$

for some fixed vector $\boldsymbol{\chi} \in (\mathbb{F}_d)^2$.

We refer to the matrices in $\mathrm{SL}(2, \mathbb{F}_d)$ as symplectic matrices.

Let us sketch the proof of these statements. It is easily seen that $\langle F\mathbf{u}, F\mathbf{v} \rangle = \mathrm{tr}\big(\det F(u_2 v_1 - u_1 v_2)\big)$. In view of Eq. (25) this means

$$2h(\mathbf{u}+\mathbf{v}) - 2h(\mathbf{u}) - 2h(\mathbf{v}) = \mathrm{tr}\big((\det F - 1)(u_2 v_1 - u_1 v_2)\big) \tag{32}$$

(mod p). Interchanging $\mathbf{u}$ and $\mathbf{v}$ we also have

$$2h(\mathbf{u}+\mathbf{v}) - 2h(\mathbf{u}) - 2h(\mathbf{v}) = -\mathrm{tr}\big((\det F - 1)(u_2 v_1 - u_1 v_2)\big) \tag{33}$$

(mod p). It follows that $\det F = 1$. Setting $\det F = 1$ in Eq. (32) we deduce that h is p-linear. In terms of the dual bases introduced earlier we have

$$\mathbf{u} = (u_1, u_2) = \sum_{r=1}^{n} \big(u_{1r}(e_r, 0) + u_{2r}(0, e_r)\big) \tag{34}$$

where $u_{jr} = \mathrm{tr}(u_j \bar{e}_r)$. So if we define

$$\boldsymbol{\chi} = \left(-\sum_{r=1}^{n} h\big((0, e_r)\big)\bar{e}_r, \sum_{r=1}^{n} h\big((e_r, 0)\big)\bar{e}_r \right) \tag{35}$$

it follows from the p-linearity of h that

$$h(\mathbf{u}) = \langle \boldsymbol{\chi}, \mathbf{u} \rangle \tag{36}$$

This establishes that for every $U \in \mathcal{C}_d^{\mathrm{r}}$ there is a matrix $F \in \mathrm{SL}(2, \mathbb{F}_d)$ and vector $\boldsymbol{\chi} \in (\mathbb{F}_d)^2$ such that

$$U D_{\mathbf{u}} U^\dagger = \omega^{\langle \boldsymbol{\chi}, \mathbf{u} \rangle} D_{F\mathbf{u}} \tag{37}$$

for all $\mathbf{u}$. The converse is also true: for each F and $\boldsymbol{\chi}$ there is a corresponding $U \in \mathcal{C}_d^{\mathrm{r}}$. In fact, it can be shown that for each $F \in \mathrm{SL}(2, \mathbb{F}_d)$ there is a unitary U_F such that

$$U_F D_{\mathbf{u}} U_F^\dagger = D_{F\mathbf{u}} \tag{38}$$

(in Section 3 we will give an explicit formula for U_F). So the unitary $U = U_F D_{\boldsymbol{\chi}}$ will transform the displacement operators according to the prescription of Eq. (37). Moreover it is easily seen, in view of the irreducibility of the standard representation of $\mathcal{W}_d$ and Schur's lemma, that if U' is any other unitary satisfying Eq. (37) then $U' = e^{i\theta} U$ for some phase $e^{i\theta}$. In short $\mathcal{C}_d^{\mathrm{r}}$ consists of the set of unitaries of the form

$$e^{i\theta} U_F D_{\boldsymbol{\chi}} \tag{39}$$

for arbitrary $F \in \mathrm{SL}(2, \mathbb{F}_d)$, $\boldsymbol{\chi} \in (\mathbb{F}_d)^2$, $\theta \in \mathbb{R}$. The properties of the displacement operators are easily understood, so in the remainder of this paper most of the work will go into understanding the properties of the symplectic unitaries U_F.

It is also interesting, and for our purposes important, to consider anti-unitary operators U with the property

$$U D_{\mathbf{u}} U^\dagger = e^{ig(\mathbf{u})} D_{f(\mathbf{u})} \tag{40}$$

for all $\mathbf{u}$ and suitable functions f, g. As before the fact that $D_{\mathbf{u}}^p = 1$ means that $e^{ig(\mathbf{u})}$ must be a pth root of unity. So we must have

$$UD_{\mathbf{u}}U^\dagger = \omega^{h(\mathbf{u})}D_{f(\mathbf{u})} \tag{41}$$

We will refer to such operators as anti-Clifford anti-unitaries. The group which consists of the Clifford unitaries $\in \mathcal{C}_d$ together with the anti-Clifford anti-unitaries just defined we will call the extended (Galoisian) Clifford group $\mathcal{E}_d$.

The description of $\mathcal{E}_d$ parallels the discussion in Section 4 of ref. [12]. Let J be the matrix

$$J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{42}$$

(so $\det J = -1$) and let U_J be the anti-unitary which acts by complex conjugation in the standard basis:

$$U_J \left(\sum_{x \in \mathbb{F}_d} c_x |x\rangle \right) = \sum_{x \in \mathbb{F}_d} c_x^* |x\rangle \tag{43}$$

Then it is easily seen that

$$U_J D_{\mathbf{u}} U_J^\dagger = D_{J\mathbf{u}} \tag{44}$$

for all $\mathbf{u}$. Now consider the unitary operator $V = UU_J$. We have

$$VD_{\mathbf{u}}V^\dagger = \omega^{h(J\mathbf{u})}D_{f(J\mathbf{u})} \tag{45}$$

implying that $V \in \mathcal{C}_d$. Conversely, if $V \in \mathcal{C}_d$ then VU_J is an anti-Clifford anti-unitary. So $\mathcal{E}_d$ is the disjoint union

$$\mathcal{E}_d = \mathcal{C}_d \cup \left(\mathcal{C}_d U_J \right) \tag{46}$$

In this paper we will be concerned, not with the full group $\mathcal{E}_d$, but with the subgroup

$$\mathcal{E}_d^{\text{r}} = \mathcal{C}_d^{\text{r}} \cup \left(\mathcal{C}_d^{\text{r}} U_J \right) \tag{47}$$

We accordingly define $\text{ESL}(2, \mathbb{F}_d)$ to be the group consisting of all 2×2 matrices with entries in $\mathbb{F}_d$ and determinant $= \pm 1$. We refer to the matrices in $\text{ESL}(2, \mathbb{F}_d)$ with determinant $= -1$ as anti-symplectic matrices. If $\det F = 1$ let U_F be the unitary defined earlier, while if $\det F = -1$ let it be the anti-unitary

$$U_F = U_{FJ}U_J \tag{48}$$

Then it is easily seen that $\mathcal{E}_d^{\text{r}}$ consists of all operators of the form

$$U = e^{i\theta}U_F D_{\boldsymbol{\chi}} \tag{49}$$

with $F \in \text{ESL}(2, \mathbb{F}_d)$, $\boldsymbol{\chi} \in (\mathbb{F}_d)^2$ and $e^{i\theta}$ an arbitrary phase. If $\det F = 1$ then U is a Clifford unitary; if $\det F = -1$ then it is an anti-Clifford anti-unitary. In either case

$$UD_{\mathbf{u}}U^\dagger = \omega^{\langle \boldsymbol{\chi}, \mathbf{u} \rangle} D_{F\mathbf{u}} \tag{50}$$

for all $\mathbf{u}$.

3. Faithful Representation of $\mathrm{ESL}(2, \mathbb{F}_d)$

Let F_1, F_2 be any two elements of $\mathrm{ESL}(2, \mathbb{F}_d)$. Then

$$U_{F_1} U_{F_2} D_{\mathbf{u}} U_{F_2}^\dagger U_{F_1}^\dagger = D_{F_1 F_2 \mathbf{u}} = U_{F_1 F_2} D_{\mathbf{u}} U_{F_1 F_2}^\dagger \tag{51}$$

for all $\mathbf{u}$. It follows from the irreducibility of the standard representation of $\mathcal{W}_d$ and Schur's lemma that

$$U_{F_1} U_{F_2} = e^{i\theta} U_{F_1 F_2} \tag{52}$$

for some phase $e^{i\theta}$, meaning that the map $F \to U_F$ is a projective representation of the group $\mathrm{ESL}(2, \mathbb{F}_d)$ (the metaplectic representation [4, 22]). In this section we show that it is possible to choose the phases of the operators U_F in such a way that the representation becomes, not merely projective, but faithful, so that

$$U_{F_1} U_{F_2} = U_{F_1 F_2} \tag{53}$$

for all F_1, F_2. The fact that this is possible for the unitaries corresponding to the elements of $\mathrm{SL}(2, \mathbb{F}_d)$ has been shown by Neuhauser [4]. We improve on his result by (a) showing that it extends to the whole of the group $\mathrm{ESL}(2, \mathbb{F}_d)$ and (b) giving explicit formulae which enable one easily to calculate the unitary/anti-unitary corresponding to an arbitrary element of $\mathrm{ESL}(2, \mathbb{F}_d)$.

We begin by establishing some preliminary results. Let $\mathbb{F}_d^*$ (respectively $\mathbb{Z}_p^*$) be the set of non-zero elements of $\mathbb{F}_d$ (respectively $\mathbb{Z}_p$). Let θ be a primitive element for the field $\mathbb{F}_d$, and for each $x \in \mathbb{F}_d^*$ let $\log_\theta x$ be the unique integer in the interval $[0, d-2]$ with the property

$$x = \theta^{\log_\theta x} \tag{54}$$

Let Q (respectively N) denote the set of quadratic residues (respectively non-quadratic residues) of $\mathbb{F}_d$:

$$Q = \{x \in \mathbb{F}_d^* : x = y^2 \text{ for some } y \in \mathbb{F}_d\} \tag{55}$$

$$N = \{x \in \mathbb{F}_d^* : x \neq y^2 \text{ for all } y \in \mathbb{F}_d\} \tag{56}$$

Clearly $x \in Q$ (respectively $x \in N$) if and only if $\log_\theta x$ is even (respectively odd). Consequently Q and N each contain exactly $(d-1)/2$ elements. Let $l(x)$ be the quadratic character of $\mathbb{F}_x$

$$l(x) = \begin{cases} 1 & x \in Q \\ -1 & x \in N \\ 0 & x = 0 \end{cases} \tag{57}$$

and let $l_p(z)$ be the quadratic character of $\mathbb{Z}_p$ (*i.e.* the Legendre symbol $\left(\frac{z}{p}\right)$). Note that l, like l_p, is multiplicative: $l(xy) = l(x)l(y)$ for all $x, y \in \mathbb{F}_d^*$. We then have the following result

Lemma 1. *Suppose $z \in \mathbb{Z}_p^*$. Then*

$$l(z) = \begin{cases} 1 & \text{if } d \text{ is an even power of } p \\ l_p(z) & \text{if } d \text{ is an odd power of } p \end{cases} \tag{58}$$

Proof. Define

$$\epsilon = \theta^{\frac{d-1}{p-1}} = \theta^{1+p+\cdots+p^{n-1}} \tag{59}$$

Then $\epsilon^p = \epsilon$, implying that $\epsilon \in \mathbb{Z}_p$. Moreover $\epsilon^r = 1$ if and only if $r = 0$ (mod $p-1$), implying that ϵ has multiplicative order $p-1$. So ϵ is a primitive element for $\mathbb{Z}_p$. By construction

$$\log_\theta z = (1 + p + \cdots + p^{n-1}) \log_\epsilon z \tag{60}$$

for all $z \in \mathbb{Z}_p^*$. If n is even then $(1 + p + \cdots + p^{n-1})$ is even, implying that $\log_\theta z$ is even for all $z \in \mathbb{Z}_p^*$. Consequently $l(z) = 1$ for all $z \in \mathbb{Z}_p^*$. If, on the other hand, n is odd then $(1 + p + \cdots + p^{n-1})$ is odd, implying that $\log_\theta z$ is even if and only if $\log_\epsilon z$ is even. Consequently $l(z) = l_p(z)$ for all $z \in \mathbb{Z}_p^*$. $\square$

It is also convenient to define the quantity

$$\tilde{l}(x) = \begin{cases} -i^{-\frac{n(p+3)}{2}} l(x) & x \neq 0 \\ 1 & x = 0 \end{cases} \tag{61}$$

It has the property

Lemma 2. *For all $x \in \mathbb{F}_d$*

$$\left(\tilde{l}(x)\right)^* = \tilde{l}(-x) \tag{62}$$

Proof. Suppose d is an even power of p. Then it follows from Lemma 1 that $l(-1) = 1$. Consequently $l(-x) = l(-1)l(x) = l(x)$. Moreover, the fact that n and $p+3$ are both even means that $i^{\frac{n(p+3)}{2}}$ is real. The claim is now immediate.

Suppose, on the other hand, that d is an odd power of p. Then in view of Lemma 1 and a standard result of number theory (see, for example, Hardy and Wright [83]) we have

$$l(-x) = l_p(-1)l(x) = (-1)^{\frac{p+3}{2}} l(x) = (-1)^{-\frac{n(p+3)}{2}} l(x) = i^{-n(p+3)} l(x) \tag{63}$$

The claim now follows. $\square$

We will also need the following Gaussian sum formula

Lemma 3. *For all $a \in \mathbb{F}_d^*$ and $b \in \mathbb{F}_d$*

$$\sum_{x \in \mathbb{F}_d} \tau^{\mathrm{tr}(ax^2 + bx)} = \sqrt{d}\, \tilde{l}(a) \tau^{-\mathrm{tr}\left(\frac{b^2}{4a}\right)} \tag{64}$$

Remark. The fact that we work in terms of τ rather than ω means that we can give a single formula which covers both the cases $p = \pm 1$ (mod 4).

Proof. Using Theorem 5.15 in Lidl and Niederreiter [82] in conjunction with the fact that $\sum_{x \in \mathbb{F}_d} \omega^{\mathrm{tr}(x)} = 0$ we find

$$\sum_{x \in \mathbb{F}_d} \omega^{\mathrm{tr}(ax^2)} = \begin{cases} 1 + 2\sum_{x \in Q} \omega^{\mathrm{tr}(x)} & \text{if } a \in Q \\ 1 + 2\sum_{x \in N} \omega^{\mathrm{tr}(x)} & \text{if } a \in N \end{cases} \tag{65}$$

$$= l(a) \sum_{x \in \mathbb{F}_d} l(x)\omega^{\mathrm{tr}(x)} \tag{66}$$

$$= \begin{cases} (-1)^{n-1} l(a)\sqrt{d} & p = 1 \ (\mathrm{mod}\ 4) \\ (-1)^{n-1} i^n l(a)\sqrt{d} & p = -1 \ (\mathrm{mod}\ 4) \end{cases} \tag{67}$$

Since $(d+1)/2$ is the multiplicative inverse of 2 considered as an element of $\mathbb{Z}_p$ we have $\tau^{\text{tr}(ax^2)} = \omega^{\text{tr}(ax^2/2)}$ and, consequently,

$$\sum_{x \in \mathbb{F}_d} \tau^{\text{tr}(ax^2)} = \begin{cases} (-1)^{n-1} l(a/2)\sqrt{d} & p = 1 \ (\text{mod } 4) \\ (-1)^{n-1} i^n l(a/2)\sqrt{d} & p = -1 \ (\text{mod } 4) \end{cases} \tag{68}$$

Suppose, now, that n is even. Then it follows from Lemma 1 that $l(a/2) = l(a)$. Moreover

$$\tilde{l}(a) = \begin{cases} (-1)^{n-1} l(a) & p = 1 \ (\text{mod } 4) \\ (-1)^{n-1} i^n l(a) & p = -1 \ (\text{mod } 4) \end{cases} \tag{69}$$

Consequently

$$\sum_{x \in \mathbb{F}_d} \tau^{\text{tr}(ax^2)} = \sqrt{d}\tilde{l}(a) \tag{70}$$

irrespective of the value of p.

Suppose, on the other hand, that n is odd. Then it follows from Lemma 1 and a standard result of number theory (see, for example, Hardy and Wright [83]) that

$$l(a/2) = l_p(2)l(a) = \begin{cases} l(a) & p = \pm 1 \ (\text{mod } 8) \\ -l(a) & p = \pm 3 \ (\text{mod } 8) \end{cases} \tag{71}$$

So

$$\sum_{x \in \mathbb{F}_d} \tau^{\text{tr}(ax^2)} = \begin{cases} l(a)\sqrt{d} & p = 1 \ (\text{mod } 8) \\ -i^n l(a)\sqrt{d} & p = 3 \ (\text{mod } 8) \\ -l(a)\sqrt{d} & p = 5 \ (\text{mod } 8) \\ i^n l(a)\sqrt{d} & p = 7 \ (\text{mod } 8) \end{cases} \tag{72}$$

Comparing with the definition of $\tilde{l}(a)$ we again find

$$\sum_{x \in \mathbb{F}_d} \tau^{\text{tr}(ax^2)} = \sqrt{d}\tilde{l}(a) \tag{73}$$

irrespective of the value of p.

Finally, if $b \neq 0$, we have

$$\sum_{x \in \mathbb{F}_d} \tau^{\text{tr}(ax^2 + bx)} = \sum_{x \in \mathbb{F}_d} \tau^{\text{tr}\left(a\left(x + \frac{b}{2a}\right)^2\right) - \frac{b^2}{4a}} = \sqrt{d}\tilde{l}(a)\tau^{-\text{tr}\left(\frac{b^2}{4a}\right)} \tag{74}$$

$\square$

We are now ready to establish the main result of this section. Let

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{75}$$

be any matrix $\in \text{ESL}(2, \mathbb{F}_d)$. If $\det F = 1$ define

$$U_F = \begin{cases} l(\alpha) \sum_{x \in \mathbb{F}_d} \tau^{\text{tr}(\alpha\gamma x^2)} |\alpha x\rangle\langle x| & \text{if } \beta = 0 \\ \frac{\tilde{l}(-\beta)}{\sqrt{d}} \sum_{x,y \in \mathbb{F}_d} \tau^{\text{tr}\left(\beta^{-1}(\alpha y^2 - 2xy + \delta x^2)\right)} |x\rangle\langle y| & \text{if } \beta \neq 0 \end{cases} \tag{76}$$

If, on the other hand, $\det F = -1$ define

$$U_F = U_{FJ}U_J \tag{77}$$

where U_{FJ} is the unitary defined by Eq. (76), J is the anti-symplectic defined by Eq. (42), and U_J is the anti-unitary defined by Eq. (43) (note that $\det(FJ) = 1$, so this definition makes sense).

We have

Theorem 4. *For all $F \in \mathrm{ESL}(2, \mathbb{F}_d)$ the operator U_F is unitary if $\det F = 1$ and anti-unitary if $\det F = -1$. We have*

(1) *For all $F \in \mathrm{ESL}(2, \mathbb{F}_d)$ and $\mathbf{u} \in \mathbb{F}_d^2$*

$$U_F D_{\mathbf{u}} U_F^\dagger = D_{F\mathbf{u}} \tag{78}$$

(2) *For all $F, F' \in \mathrm{ESL}(2, \mathbb{F}_d)$*

$$U_F U_{F'} = U_{FF'} \tag{79}$$

$$U_{F^{-1}} = U_F^\dagger \tag{80}$$

Proof. Suppose, first of all, that $\det F = 1$ and $\beta = 0$. Then

$$U_F D_{\mathbf{u}} U_F^\dagger = \sum_{x,y \in \mathbb{F}_d} \tau^{\mathrm{tr}(\alpha\gamma(x^2-y^2))} \langle x|D_{\mathbf{u}}|y\rangle |\alpha x\rangle\langle \alpha y| \tag{81}$$

$$= \sum_{x,y \in \mathbb{F}_d} \tau^{\mathrm{tr}(\alpha^{-1}\gamma(x^2-y^2))} \tau^{\mathrm{tr}(u_1 u_2 + 2\alpha^{-1}u_2 y)} \delta_{x,y+\alpha u_1} |x\rangle\langle y| \tag{82}$$

$$= \sum_{x,y \in \mathbb{F}_d} \tau^{\mathrm{tr}(\alpha u_1(\gamma u_1 + \delta u_2))} \omega^{\mathrm{tr}((\gamma u_1 + \delta u_2)y)} |y + \alpha u_1\rangle\langle y| \tag{83}$$

$$= D_{F\mathbf{u}} \tag{84}$$

which establishes Eq. (78) for this case. Setting $\mathbf{u} = \mathbf{0}$ we also see that U_F is unitary.

Suppose, next, that $\det F = 1$ and $\beta \neq 0$. Then

$$U_F D_{\mathbf{u}} U_F^\dagger = \frac{1}{d} \sum_{\substack{x_1,x_2, \\ y_1,y_2 \in \mathbb{F}_d}} \tau^{\mathrm{tr}(\beta^{-1}(\alpha(y_1^2-y_2^2)-2(x_1 y_1 - x_2 y_2)+\delta(x_1^2-x_2^2)))} \langle y_1|D_{\mathbf{u}}|y_2\rangle |x_1\rangle\langle x_2|$$

$$= \frac{1}{d} \sum_{\substack{x_1,x_2, \\ y_1,y_2 \in \mathbb{F}_d}} \tau^{\mathrm{tr}(\beta^{-1}(\alpha(y_1^2-y_2^2)-2(x_1 y_1 - x_2 y_2)+\delta(x_1^2-x_2^2))+u_1 u_2 + 2 u_2 y_2)}$$

$$\times \delta_{y_1,y_2+u_1} |x_1\rangle\langle x_2|$$

$$= \sum_{x_1,x_2 \in \mathbb{F}_d} \left(\frac{1}{d} \sum_{y_2 \in \mathbb{F}_d} \tau^{\mathrm{tr}(-2\beta^{-1}(x_1 - x_2 - \alpha u_1 - \beta u_2)y_2)} \right)$$

$$\times \tau^{\mathrm{tr}(\beta^{-1}(\delta(x_1^2-x_2^2)-2u_1 x_1 + \alpha u_1^2 + \beta u_1 u_2))} |x_1\rangle\langle x_2|$$

$$= \sum_{x_1,x_2 \in \mathbb{F}_d} \tau^{\mathrm{tr}(\beta^{-1}(\delta(x_1^2-x_2^2)-2u_1 x_1 + \alpha u_1^2 + \beta u_1 u_2))} \delta_{x_1,x_2+\alpha u_1 + \beta u_2} |x_1\rangle\langle x_2|$$

$$= \sum_{x \in \mathbb{F}_d} \tau^{\mathrm{tr}((\alpha u_1 + \beta u_2)(\gamma u_1 + \delta u_2))} \omega^{\mathrm{tr}((\gamma u_1 + \delta u_2)x)} |x + \alpha u_1 + \beta u_2\rangle\langle x|$$

$$= D_{F\mathbf{u}} \tag{85}$$

which establishes Eq. (78) and the fact that U_F is unitary for this case also.

It remains to consider the case when $\det F = -1$. We have

$$U_J D_{\mathbf{u}} U_J^\dagger = D_{J\mathbf{u}} \tag{86}$$

In view of the foregoing it follows that

$$U_F D_{\mathbf{u}} U_F^\dagger = U_{FJ} U_J D_{\mathbf{u}} U_J^\dagger U_{FJ}^\dagger = D_{F\mathbf{u}} \tag{87}$$

We now turn to the proof that the representation is faithful. Let

$$F_1 = \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} \qquad\qquad F_2 = \begin{pmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{pmatrix} \tag{88}$$

be two matrices $\in \mathrm{ESL}(2, \mathbb{F}_d)$, and let

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{89}$$

be the product $F_1 F_2$.

To start with suppose that $\det F_1 = \det F_2 = 1$. There are four cases to consider

Case 1. $\beta_1 = \beta_2 = 0$. Then

$$
\begin{aligned}
U_{F_1} U_{F_2} &= l(\alpha_1 \alpha_2) \sum_{x_1, x_2 \in \mathbb{F}_d} \tau^{\mathrm{tr}(\alpha_1 \gamma_1 x_1^2 + \alpha_2 \gamma_2 x_2^2)} \delta_{x_1, \alpha_2 x_2} |\alpha_1 x_1\rangle\langle x_2| \\
&= l(\alpha) \sum_{x \in \mathbb{F}_d} \tau^{\mathrm{tr}(\alpha \gamma x^2)} |\alpha x\rangle\langle x| \\
&= U_F \tag{90}
\end{aligned}
$$

Case 2. $\beta_1 = 0$, $\beta_2 \neq 0$. Then

$$
\begin{aligned}
U_{F_1} U_{F_2} &= \frac{l(\alpha_1)\tilde{l}(-\beta_2)}{\sqrt{d}} \sum_{\substack{x_1, x_2, \\ y_2 \in \mathbb{F}_d}} \tau^{\mathrm{tr}(\alpha_1 \gamma_1 x_1^2 + \beta_2^{-1}(\alpha_2 y_2^2 - 2x_2 y_2 + \delta_2 x_2^2))} \delta_{x_1, x_2} |\alpha_1 x_1\rangle\langle y_2| \\
&= \frac{\tilde{l}(-\alpha_1 \beta_2)}{\sqrt{d}} \sum_{x, y \in \mathbb{F}_d} \tau^{\mathrm{tr}\left(\alpha_1^{-1}\beta_2^{-1}\left((\gamma_1 \beta_2 + \delta_1 \delta_2)x^2 - 2xy + \alpha_1 \alpha_2 y^2\right)\right)} |x\rangle\langle y| \\
&= \frac{\tilde{l}(-\beta)}{\sqrt{d}} \sum_{x, y \in \mathbb{F}_d} \tau^{\mathrm{tr}(\beta^{-1}(\delta x^2 - 2xy + \alpha y^2))} |x\rangle\langle y| \\
&= U_F \tag{91}
\end{aligned}
$$

Case 3. $\beta_1 \neq 0$, $\beta_2 = 0$. The proof is similar to that of Case 2.

Case 4. $\beta_1 \neq 0$, $\beta_2 \neq 0$. Then

$$
\begin{aligned}
U_{F_1} U_{F_2} &= \frac{\tilde{l}(-\beta_1)\tilde{l}(-\beta_2)}{d} \sum_{\substack{x_1, x_2, \\ y_1, y_2 \in \mathbb{F}_d}} \tau^{\mathrm{tr}\left(\beta_1^{-1}(\alpha_1 y_1^2 - 2x_1 y_1 + \delta_1 x_1^2) + \beta_2^{-1}(\alpha_2 y_2^2 - 2x_2 y_2 + \delta_2 x_2^2)\right)} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \times \delta_{y_1, x_2} |x_1\rangle\langle y_2| \\
&= \frac{\tilde{l}(-\beta_1)\tilde{l}(-\beta_2)}{d} \sum_{x, y \in \mathbb{F}_d} \left(\sum_{z \in \mathbb{F}_d} \tau^{\mathrm{tr}\left(\beta_1^{-1}\beta_2^{-1}\beta z^2 - 2(\beta_1^{-1}x + \beta_2^{-1}y)z\right)} \right) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\quad \times \tau^{\mathrm{tr}(\beta_1^{-1}\delta_1 x^2 + \beta_2^{-1}\alpha_2 y^2)} |x\rangle\langle y| \tag{92}
\end{aligned}
$$

It follows from Lemma 3 that

$$\sum_{z \in \mathbb{F}_d} \tau^{\mathrm{tr}\left(\beta_1^{-1}\beta_2^{-1}\beta z^2 - 2(\beta_1^{-1}x + \beta_2^{-1}y)z\right)}$$

$$= \begin{cases} d\delta_{x,-\beta_1\beta_2^{-1}y} & \beta = 0 \\ \sqrt{d}\tilde{l}(\beta_1^{-1}\beta_2^{-1}\beta)\tau^{-\operatorname{tr}\left(\beta^{-1}\beta_1\beta_2(\beta_1^{-1}x+\beta_2^{-1}y)^2\right)} & \beta \neq 0 \end{cases} \quad (93)$$

So if $\beta = 0$

$$U_{F_1}U_{F_2} = \tilde{l}(-\beta_1)\tilde{l}(-\beta_2)\sum_{y\in\mathbb{F}_d}\tau^{\operatorname{tr}\left(\beta_1\beta_2^{-1}(\beta_2^{-1}\delta_1+\beta_1^{-1}\alpha_2)y^2\right)}|-\beta_1\beta_2^{-1}y\rangle\langle y| \quad (94)$$

To evaluate this expression observe that if $\beta = 0$

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ \gamma & \alpha^{-1} \end{pmatrix}\begin{pmatrix} \delta_2 & -\beta_2 \\ -\gamma_2 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha\delta_2 & -\alpha\beta_2 \\ \gamma\delta_2 - \alpha^{-1}\gamma_2 & -\beta_2\gamma + \alpha^{-1}\alpha_2 \end{pmatrix} \quad (95)$$

from which it is easily seen that

$$\alpha = -\beta_1\beta_2^{-1} \quad (96)$$

$$\gamma = -\beta_2^{-1}\delta_1 - \beta_1^{-1}\alpha_2 \quad (97)$$

Also, in view of Lemma 2,

$$\tilde{l}(-\beta_1)\tilde{l}(-\beta_2) = \tilde{l}(-\beta_1)\left(\tilde{l}(\beta_2)\right)^* = l(-\beta_1\beta_2) = l(-\beta_1\beta_2^{-1}) = l(\alpha) \quad (98)$$

Substituting these expressions into Eq. (94) we deduce

$$U_{F_1}U_{F_2} = l(\alpha)\sum_{y\in\mathbb{F}_d}\tau^{\operatorname{tr}(\alpha\gamma y^2)}|\alpha y\rangle\langle y| = U_F \quad (99)$$

Suppose, on the other hand, that $\beta = 0$. Then Eq. (92) becomes

$$U_{F_1}U_{F_2} = \frac{1}{\sqrt{d}}\tilde{l}(-\beta_1)\tilde{l}(-\beta_2)\tilde{l}(\beta_1^{-1}\beta_2^{-1}\beta)$$

$$\times \sum_{x,y\in\mathbb{F}_d}\tau^{\operatorname{tr}\left(\beta^{-1}\left(\beta_2^{-1}(\beta\alpha_2-\beta_1)y^2-2xy+\beta_1^{-1}(\beta\delta_1-\beta_2)x^2\right)\right)}|x\rangle\langle y| \quad (100)$$

To evaluate this expression observe that

$$\beta\alpha_2 - \beta_1 = \beta_2\alpha \quad (101)$$

$$\beta\delta_1 - \beta_2 = \beta_1\delta \quad (102)$$

Also

$$\tilde{l}(-\beta_1)\tilde{l}(-\beta_2)\tilde{l}(\beta_1^{-1}\beta_2^{-1}\beta) = \tilde{l}(-\beta_1)\tilde{l}(-\beta_2)\left(\tilde{l}(-\beta_1^{-1}\beta_2^{-1}\beta)\right)^*$$

$$= -i^{-\frac{n(p+3)}{2}}l(-\beta_1)l(-\beta_2)l(-\beta_1^{-1}\beta_2^{-1}\beta)$$

$$= -i^{-\frac{n(p+3)}{2}}l(-\beta)$$

$$= \tilde{l}(-\beta) \quad (103)$$

Substituting these expressions into Eq. (100) we deduce

$$U_{F_1}U_{F_2} = \frac{\tilde{l}(-\beta)}{\sqrt{d}}\sum_{x,y\in\mathbb{F}_d}\tau^{\operatorname{tr}(\beta^{-1}(\alpha y^2-2xy+\delta x^2))}|x\rangle\langle y| = U_F \quad (104)$$

We now turn to the case when either or both of F_1, F_2 is an anti-symplectic matrix. It is readily verified that for all $F \in \operatorname{ESL}(2,\mathbb{F}_d)$

$$U_F U_J = U_{FJ} \quad (105)$$

$$U_J U_F = U_{JF} \quad (106)$$

Now let F_1 be symplectic and F_2 anti-symplectic. Then in view of the foregoing

$$U_{F_1} U_{F_2} = U_{F_1} U_{F_2} J U_J = U_{F_1 F_2} J U_J = U_{F_1 F_2} \tag{107}$$

It then follows from this and Eq. (106) that if F_1 is anti-symplectic

$$U_{F_1} U_{F_2} = U_{F_1} J U_J U_{F_2} = U_{F_1} J U_{J F_2} = U_{F_1 F_2} \tag{108}$$

for all F_2, symplectic or anti-symplectic. Finally, we note that Eq. (80) is an immediate consequence of Eq. (79) and the fact that the U_F are all unitary/ anti-unitary. $\qquad\square$

4. EXPRESSING THE U_F IN TERMS OF THE $D_{\mathbf{u}}$

In the last section we gave explicit expressions for the matrix elements of the operators U_F in the standard basis. However, it is sometimes useful to express them instead as linear combinations of the $D_{\mathbf{u}}$. The fact that this is possible is an immediate consequence of the fact that

$$\mathrm{Tr}\left(D_{\mathbf{u}}^\dagger D_{\mathbf{v}}\right) = d\delta_{\mathbf{u},\mathbf{v}} \tag{109}$$

which shows that, relative to the Hilbert-Schmidt inner-product $\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$, the operators $\frac{1}{\sqrt{d}} D_{\mathbf{u}}$ are an orthonormal basis for the space of linear operators on d-dimensional Hilbert space (note that we use the symbol Tr for the ordinary matrix trace, and tr for the field-theoretic trace). The following theorem gives the relevant formulae.

Theorem 5. *Let*

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{110}$$

be any matrix $\in \mathrm{SL}(2, \mathbb{F}_d)$ *(so* $\det F = 1$*). Let* $t = \mathrm{Tr}(F)$*. Then*
    (a) *If* $t \neq 2$

$$U_F = \begin{cases} \frac{l(t-2)}{d} \sum_{\mathbf{u}\in\mathbb{F}_d^2} \tau^{\langle \mathbf{u}, \tilde{F}\mathbf{u}\rangle} D_{\mathbf{u}} & \beta \neq 0 \\ \frac{l(\alpha)}{d} \sum_{\mathbf{u}\in\mathbb{F}_d^2} \tau^{\langle \mathbf{u}, \tilde{F}\mathbf{u}\rangle} D_{\mathbf{u}} & \beta = 0 \end{cases} \tag{111}$$

where

$$\tilde{F} = \frac{1}{2-t} F \tag{112}$$

    (b) *If* $t = 2$

$$U_F = \begin{cases} \frac{\tilde{l}(-\beta)}{\sqrt{d}} \sum_{r\in\mathbb{F}_d} \tau^{\mathrm{tr}(\beta r^2)} D_{\beta r,(1-\alpha)r} & \beta \neq 0 \\ \frac{\tilde{l}(\gamma)}{\sqrt{d}} \sum_{r\in\mathbb{F}_d} \tau^{-\mathrm{tr}(\gamma r^2)} D_{0,\gamma r} & \beta = 0 \text{ and } \gamma \neq 0 \\ D_{\mathbf{0}} & \beta = \gamma = 0 \end{cases} \tag{113}$$

We also have
    (c) *If* $t \neq 2$

$$\mathrm{Tr}\left(U_F\right) = \begin{cases} l(t-2) & \beta \neq 0 \\ l(\alpha) & \beta = 0 \end{cases} \tag{114}$$

    (d) *If* $t = 2$

$$\mathrm{Tr}(U_F) = \begin{cases} \tilde{l}(-\beta)\sqrt{d} & \beta \neq 0 \\ \tilde{l}(\gamma)\sqrt{d} & \beta = 0 \text{ and } \gamma \neq 0 \\ d & \beta = \gamma = 0 \end{cases} \tag{115}$$

Proof. Suppose that $\beta = 0$. Then it follows from the definitions of $D_{\mathbf{u}}$, U_F that

$$\mathrm{Tr}\left(D_{\mathbf{u}}^{\dagger}U_F\right) = \sum_{x,y\in\mathbb{F}_d} \langle x|D_{\mathbf{u}}^{\dagger}|y\rangle\langle y|U_F|x\rangle$$

$$= l(\alpha)\sum_{x,y\in\mathbb{F}_d} \tau^{\mathrm{tr}\left(\alpha\gamma x^2 - 2u_2 y + u_1 u_2\right)}\delta_{x,y-u_1}\delta_{y,\alpha x}$$

$$= \begin{cases} l(\alpha)\tau^{\langle\mathbf{u},\tilde{F}\mathbf{u}\rangle} & t \neq 2 \\ \sqrt{d}\tilde{l}(\gamma)\tau^{-\,\mathrm{tr}(\gamma^{-1}u_2^2)}\delta_{u_1,0} & t = 2 \text{ and } \gamma \neq 0 \\ d\delta_{\mathbf{u},\mathbf{0}} & t = 2 \text{ and } \gamma = 0 \end{cases} \qquad (116)$$

where we used Lemma 3 in the last line. Suppose, on the other hand, that $\beta \neq 0$. Then

$$\mathrm{Tr}\left(D_{\mathbf{u}}^{\dagger}U_F\right) = \sum_{x,y\in\mathbb{F}_d} \langle x|D_{\mathbf{u}}^{\dagger}|y\rangle\langle y|U_F|x\rangle$$

$$= \frac{1}{\sqrt{d}}\tilde{l}(-\beta)\sum_{x,y\in\mathbb{F}_d} \tau^{\mathrm{tr}\left(\beta^{-1}(\alpha x^2 - 2xy + \delta y^2) - 2u_2 y + u_1 u_2\right)}\delta_{x,y-u_1}$$

$$= \frac{1}{\sqrt{d}}\tilde{l}(-\beta)\sum_{x\in\mathbb{F}_d} \tau^{\mathrm{tr}\left(\beta^{-1}(t-2)x^2 + 2(\beta^{-1}(\delta-1)u_1 - u_2)x + \beta^{-1}\delta u_1^2 - u_1 u_2\right)}$$

$$= \begin{cases} l(t-2)\tau^{\langle\mathbf{u},\tilde{F}\mathbf{u}\rangle} & t \neq 2 \\ \sqrt{d}\tilde{l}(-\beta)\tau^{\mathrm{tr}(\beta^{-1}u_1^2)}\delta_{u_2,\beta^{-1}(1-\alpha)u_1} & t = 2 \end{cases} \qquad (117)$$

where we again used Lemma 3. Statements (c) and (d) of the theorem are special cases of these formulae (since $D_{\mathbf{0}} = 1$). Statements (a) and (b) are immediate consequences of them and the fact

$$U_F = \frac{1}{d}\sum_{\mathbf{u}\in\mathbb{F}_d^2} \mathrm{Tr}\left(D_{\mathbf{u}}^{\dagger}U_F\right)D_{\mathbf{u}} \qquad (118)$$

□

5. Eigenvalues and Orders of the (anti-)Symplectic Matrices

We now turn to the problem of calculating the eigenvalues and order of an arbitrary symplectic/anti-symplectic matrix

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad (119)$$

Once these are known it is straightforward to find the order, the eigenvalues and eigenspaces and the roots of the corresponding unitary/anti-unitary U_F.

Let $t = \alpha + \delta$ be the trace (in the ordinary matrix sense) of F, and let Δ be its determinant. We say that F is

(1) type 1 if $t^2 - 4\Delta \in Q$
(2) type 2 if $t^2 - 4\Delta \in N$
(3) type 3 if $t^2 - 4\Delta = 0$.

Suppose, to begin with, that F is type 1. Then F is conjugate to the matrix [23, 28, 84, 85]

$$\bar{F} = \begin{pmatrix} 0 & -\Delta \\ 1 & t \end{pmatrix} \qquad (120)$$

This matrix is diagonalizable. In fact

$$\det(F - \lambda I) = \lambda^2 - t\lambda + \Delta \tag{121}$$

So the equation $\det(F - \lambda I) = 0$ has the two solutions

$$\lambda_\pm = \frac{t \pm \sqrt{t^2 - 4\Delta}}{2} \tag{122}$$

where $\sqrt{t^2 - 4\Delta}$ is one of the two elements of $\mathbb{F}_d$ with the property $\left(\sqrt{t^2 - 4\Delta}\right)^2 = t^2 - 4\Delta$ (guaranteed to exist because of the assumption that $t^2 - 4\Delta \in Q$) and where, as usual, division by 2 means multiplication by the multiplicative inverse of 2 considered as an element of $\mathbb{F}_d$. It is easily verified that

$$\Delta = \lambda_+ \lambda_- \tag{123}$$
$$t = \lambda_+ + \lambda_- \tag{124}$$

This means we can write

$$\lambda_+ = \theta^r \tag{125}$$
$$\lambda_- = \Delta\theta^{-r} \tag{126}$$

where $r = \log_\theta \lambda_+$. The fact that $(\Delta\theta^{-r} - \theta^r)^2 = t^2 - 4\Delta \in Q$ means that $\Delta\theta^{-r} \neq \theta^r$. So the matrix

$$S = \begin{pmatrix} \frac{\theta^{-r}}{\Delta\theta^{-r} - \theta^r} & \frac{1}{\Delta\theta^{-r} - \theta^r} \\ \Delta\theta^r & 1 \end{pmatrix} \tag{127}$$

is a well-defined element of $\mathrm{ESL}(2, \mathbb{F}_d)$. It is straightforward to confirm that

$$S\bar{F}S^{-1} = \begin{pmatrix} \theta^r & 0 \\ 0 & \Delta\theta^{-r} \end{pmatrix} \tag{128}$$

So the problem of finding the order of F reduces to the problem of finding the smallest positive integer m such that

$$\begin{pmatrix} \theta^r & 0 \\ 0 & \Delta\theta^{-r} \end{pmatrix}^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{129}$$

If $\Delta = 1$ we immediately deduce that

$$\mathrm{ord}(F) = \frac{d-1}{[r, (d-1)]} \tag{130}$$

where $[r, (d-1)]$ is the greatest common divisor of r and $d-1$. Suppose, on the other hand, that $\Delta = -1$. Then the order of F is the smallest even positive integer m such that $\theta^m = 1$. So

$$\mathrm{ord}(F) = \begin{cases} \frac{(d-1)}{[r,(d-1)]} & \text{if } \frac{(d-1)}{[r,(d-1)]} \text{ is even} \\ \frac{2(d-1)}{[r,(d-1)]} & \text{if } \frac{(d-1)}{[r,(d-1)]} \text{ is odd} \end{cases} \tag{131}$$

We can write this formula more compactly if we observe

$$\left[r, \frac{d-1}{2}\right] = \begin{cases} [r, d-1] & \text{if } \frac{(d-1)}{[r,(d-1)]} \text{ is even} \\ \frac{1}{2}[r, d-1] & \text{if } \frac{(d-1)}{[r,(d-1)]} \text{ is odd} \end{cases} \tag{132}$$

from which it follows

$$\text{ord}(F) = \frac{d-1}{[r, \frac{d-1}{2}]} \tag{133}$$

Let us note that for all r in the interval $0 \le r < d-1$ the matrix

$$\bar{F} = \begin{pmatrix} 0 & -\Delta \\ 1 & \theta^r + \Delta\theta^{-r} \end{pmatrix} \tag{134}$$

is a well-defined element of $\text{ESL}(2, \mathbb{F}_d)$. However, for some values of r the matrix is type 3 and not diagonalizable. It is easily seen that the values of r for which $\bar{F}$ is a type 1 matrix with eigenvalues θ^r, $\Delta\theta^{-r}$ are

$$\left\{ r \colon 1 \le r < d-1,\ r \ne \frac{d-1}{2} \right\} \qquad\qquad \text{if } \Delta = 1 \tag{135}$$

$$\left\{ r \colon 1 \le r < d-1,\ r \ne \frac{d-1}{4}, \frac{3(d-1)}{4} \right\} \quad \text{if } \Delta = -1 \text{ and } d = 1 \ (\text{mod } 4) \tag{136}$$

$$\{ r \colon 1 \le r < d-1 \} \qquad\qquad\qquad \text{if } \Delta = -1 \text{ and } d = 3 \ (\text{mod } 4) \tag{137}$$

In particular the maximum order of a type 1 matrix is $d-1$, the maximum being achieved by (for example) matrices for which $t = \theta + \Delta\theta^{-1}$.

Suppose, next, that F is type 2. Then F is again conjugate to the matrix [23, 28, 84, 85]

$$\bar{F} = \begin{pmatrix} 0 & -\Delta \\ 1 & t \end{pmatrix} \tag{138}$$

However the fact that the discriminant $t^2 - 4\Delta \in N$ means that the equation

$$\det(F - \lambda I) = \lambda^2 - t\lambda + \Delta = 0 \tag{139}$$

has no solutions in the field $\mathbb{F}_d$. We can deal with this problem in the same way that we would if we had a matrix defined over the reals whose characteristic equation had a negative discriminant: namely, we can go to a suitable extension field, in this case $\mathbb{F}_{d^2}$. Let $\bar{\theta}$ be a primitive element for $\mathbb{F}_{d^2}$. We make the identification

$$\mathbb{F}_d = \{ x \in \mathbb{F}_{d^2} \colon x^{d-1} = 1 \} \tag{140}$$

$\mathbb{F}_d^*$ thus consists of all powers of $\bar{\theta}^{d+1}$. It follows that $\bar{\theta}^{d+1}$ is a primitive element for $\mathbb{F}_d$ which, without loss of generality, we can identify with θ.

To define the square root of an arbitrary element $x \in N$ observe that $x = \bar{\theta}^{k(d+1)}$ for some odd integer k. So if we define $\sqrt{x} = \bar{\theta}^{\frac{k(d+1)}{2}}$ we will have $x = (\sqrt{x})^2$. Observe that, since $\bar{\theta}^{\frac{d^2-1}{2}} = -1$ and k is odd,

$$\left(\sqrt{x}\right)^d = \bar{\theta}^{\frac{k(d^2-1)}{2}} \bar{\theta}^{\frac{k(d+1)}{2}} = -\sqrt{x} \tag{141}$$

Now let

$$\lambda_\pm = \frac{t \pm \sqrt{t^2 - 4\Delta}}{2} \tag{142}$$

be the solutions of Eq. (139). Using the fact that $(x \pm y)^d = x^d \pm y^d$ for all $x, y \in \mathbb{F}_{d^2}$ we deduce

$$\lambda_\pm^d = \frac{t^d \pm \left(\sqrt{t^2 - 4\Delta}\right)^d}{2^d} \tag{143}$$

In view of Eq. (141) and the fact that $x^d = x$ for all $x \in \mathbb{F}_d$ it follows

$$\lambda_\pm^d = \lambda_\mp \tag{144}$$

So

$$\lambda_+ = \bar{\theta}^k \tag{145}$$

$$\lambda_- = \bar{\theta}^{kd} \tag{146}$$

for some integer k. Since $\lambda_+ \lambda_- = \Delta$, and taking account of the fact that $\bar{\theta}^{-\frac{d^2-1}{2}} = -1$, we must have

$$k(d+1) = \begin{cases} 0 & \text{if } \Delta = 1 \\ \frac{d^2-1}{2} & \text{if } \Delta = -1 \end{cases} \tag{147}$$

mod $(d^2 - 1)$. So if we define $\eta = \bar{\theta}^{\frac{d-1}{2}}$

$$\lambda_+ = \eta^r \tag{148}$$

$$\lambda_- = \eta^{rd} = (-1)^r \eta^{-r} \tag{149}$$

for some integer r which is in the range $1 \le r < 2(d+1)$, and which is even if $\Delta = 1$ and odd if $\Delta = -1$.

Since $t^2 - 4\Delta \ne 0$ the eigenvalues are distinct and so the matrix

$$S = \begin{pmatrix} \frac{1}{(-1)^r - \eta^{2r}} & \frac{\eta^r}{(-1)^r - \eta^{2r}} \\ (-1)^r \eta^r & 1 \end{pmatrix} \tag{150}$$

is a well-defined element of $\mathrm{ESL}(2, \mathbb{F}_{d^2})$. It is readily verified that

$$S\bar{F}S^{-1} = \begin{pmatrix} \eta^r & 0 \\ 0 & (-1)^r \eta^{-r} \end{pmatrix} \tag{151}$$

from which we see that the order of F is the smallest positive integer m such that $\eta^{mr} = 1$. Since $\eta^k = 1$ if and only if $k = 0 \pmod{2(d+1)}$ we conclude

$$\mathrm{ord}(F) = \frac{2(d+1)}{[r, 2(d+1)]} \tag{152}$$

It follows from this that every symplectic matrix has order $\le d + 1$, and every anti-symplectic matrix has order $\le 2d + 2$. Let us note that there exist both symplectic and anti-symplectic matrices which achieve these upper bounds. This is a consequence of the more general fact that for every value of r in the interval $1 \le r < 2(d+1)$ there is a matrix $F \in \mathrm{ESL}(2, \mathbb{F}_d)$ with eigenvalues $\eta^r, (-1)^r \eta^{-r}$. To prove this observe

$$\left(\eta^r + (-1)^r \eta^{-r} \right)^d = \eta^{dr} + (-1)^r \eta^{-dr} = \eta^r + (-1)^r \eta^{-r} \tag{153}$$

(since $\eta^{dr} = (-1)^r \eta^{-r}$), implying that $\eta^r + (-1)^r \eta^{-r} \in \mathbb{F}_d$. So the matrix

$$\bar{F} = \begin{pmatrix} 0 & (-1)^{r+1} \\ 1 & \eta^r + (-1)^r \eta^{-r} \end{pmatrix} \tag{154}$$

is in $\mathrm{ESL}(2, \mathbb{F}_d)$ and has eigenvalues $\eta^r, (-1)^r \eta^{-r}$. In particular

$$\bar{F} = \begin{pmatrix} 0 & 1 \\ -1 & \eta^2 + \eta^{-2} \end{pmatrix} \tag{155}$$

is a symplectic matrix having the maximum order $d + 1$ and

$$\bar{F} = \begin{pmatrix} 0 & 1 \\ 1 & \eta - \eta^{-1} \end{pmatrix} \tag{156}$$

is an anti-symplectic matrix having the maximum order $2(d + 1)$.

It remains to consider type 3 matrices. A type 3 matrix is not diagonalizable except in the trivial case when $F = \pm I$. We have the further complication that the conjugacy class of a type 3 matrix

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{157}$$

depends, not only on the values of t and Δ, but also on the values of β and γ. Finally, we need to consider the cases $d = 1 \pmod 4$ and $d = 3 \pmod 4$ separately. Using the results in ref. [28] we give in Table 1 a representative for each of the 12 conjugacy classes when $d = 1 \pmod 4$, while in Table 2 we give a representative for each of the 4 conjugacy classes when $d = 3 \pmod 4$. The last column in each table gives the order of the matrices in the corresponding conjugacy class, calculated using the formula

$$\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}^r = \begin{pmatrix} x^r & rx^{r-1}y \\ 0 & x^r \end{pmatrix} \tag{158}$$

We have thus proved

Theorem 6. *Let F be any element of $\mathrm{ESL}(2, \mathbb{F}_d)$. Let t be the trace of F (in the ordinary matrix sense) and let Δ be the determinant. Then*

(1) *If F is type 1 let*

$$r = \log_\theta \left(\frac{-t + \sqrt{t^2 - 4\Delta}}{2} \right) \tag{159}$$

Then the order of F is given by

$$\mathrm{ord}(F) = \begin{cases} \frac{d-1}{[r, d-1]} & \text{if } \Delta = 1 \\ \frac{d-1}{[r, \frac{d-1}{2}]} & \text{if } \Delta = -1 \end{cases} \tag{160}$$

where $[u, v]$ denotes the greatest common divisor of u and v. The allowed values of r are

$$\left\{ r : 1 \leq r < d - 1, \ r \neq \frac{d-1}{2} \right\} \qquad \text{if } \Delta = 1 \tag{161}$$

$$\left\{ r : 1 \leq r < d - 1, \ r \neq \frac{d-1}{4}, \frac{3(d-1)}{4} \right\} \quad \text{if } \Delta = -1 \text{ and } d = 1 \ (mod \ 4) \tag{162}$$

$$\{ r : 1 \leq r < d - 1 \} \qquad \text{if } \Delta = -1 \text{ and } d = 3 \ (mod \ 4) \tag{163}$$

In particular the maximum order of a type 1 matrix is $d - 1$, the maximum being achieved by (for example) symplectic matrices for which $t = \theta + \theta^{-1}$ and anti-symplectic matrices for which $t = \theta - \theta^{-1}$.

(2) *If F is type 2 let $\bar\theta$ be a primitive element of $\mathbb{F}_{d^2}$ and let $\eta = \bar\theta^{\frac{d-1}{2}}$. Define*

$$r = \log_\eta \left(\frac{-t + \sqrt{t^2 - 4\Delta}}{2} \right) \tag{164}$$

Then the order of F is given by

$$\mathrm{ord}(F) = \frac{2(d+1)}{[r, 2(d+1)]} \tag{165}$$

Every value of r in the interval $1 \leq r < 2(d + 1)$ is possible. r is even for symplectic and odd for anti-symplectic matrices. So the maximum order of

a type 2 symplectic matrix is $d+1$, the maximum being achieved by (for example) matrices for which $t = \eta^2 + \eta^{2d}$, while the maximum order for a type 2 anti-symplectic matrix is $2(d+1)$, the maximum being achieved by (for example) matrices for which $t = \eta + \eta^d$.

(3) If F is type 3 the order is as tabulated in Table 1 (if $d = 1$ (mod 4)) or Table 2 (if $d = 3$ (mod 4)).

Δ	t	β, γ	representative	order
1	2	$\beta = \gamma = 0$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1
1	2	β or $\gamma \in Q$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	p
1	2	β or $\gamma \in N$	$\begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix}$	p
1	-2	$\beta = \gamma = 0$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	2
1	-2	β or $\gamma \in Q$	$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$	2 p
1	-2	β or $\gamma \in N$	$\begin{pmatrix} -1 & \nu \\ 0 & -1 \end{pmatrix}$	2 p
-1	$2i$	$\beta = \gamma = 0$	$\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$	4
-1	$2i$	β or $\gamma \in Q$	$\begin{pmatrix} i & 1 \\ 0 & i \end{pmatrix}$	4 p
-1	$2i$	β or $\gamma \in N$	$\begin{pmatrix} i & \nu \\ 0 & i \end{pmatrix}$	4 p
-1	$-2i$	$\beta = \gamma = 0$	$\begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix}$	4
-1	$-2i$	β or $\gamma \in Q$	$\begin{pmatrix} -i & 1 \\ 0 & -i \end{pmatrix}$	4 p
-1	$-2i$	β or $\gamma \in N$	$\begin{pmatrix} -i & \nu \\ 0 & -i \end{pmatrix}$	4 p

TABLE 1. Orders of Type 3 matrices when $d = 1$ (mod 4). Here ν is any fixed element of N, and i is one of the two solutions to the equation $x^2 = -1$ (so i does *not* have its usual meaning—for instance if $d = 5$ then $i = 2$ or 4). Note, also, that it is not possible for $\beta \in Q$ and $\gamma \in N$, or for $\beta \in N$ and $\gamma \in Q$. For more details see ref. [28].

With these results in hand it is straightforward to find the order, eigenvalues and eigenspaces and roots of the unitary/anti-unitary U_F corresponding to an arbitrary

Δ	t	β, γ	representative	order
1	2	$\beta = \gamma = 0$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1
1	2	β or $\gamma \neq 0$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	p
1	-2	$\beta = \gamma = 0$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	2
1	-2	β or $\gamma \neq 0$	$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$	$2p$

TABLE 2. Orders of Type 3 matrices when $d = 3$ (mod 4). Note that for these values of d there are no type 3 anti-symplectics. For more details see ref. [28].

matrix $F \in \mathrm{ESL}(2, \mathbb{F}_d)$. In fact, let $m = \mathrm{ord}(F)$. Then m is also the order of U_F. So the eigenvalues of U_F are $e^{\frac{2ir\pi}{m}}$, with $r = 0, 1, \ldots, m-1$. The projector onto the eigenspace of U_F with eigenvalue $e^{\frac{2ir\pi}{m}}$ is

$$P_r = \frac{1}{m} \sum_{s=0}^{m-1} e^{-\frac{2irs\pi}{m}} U_F^s \qquad (166)$$

The dimension of the eigenspace (possibly zero) is $\mathrm{Tr}(P_r)$. Finally, suppose we want to find the sth roots of U_F: i.e. the set of (anti-)symplectic unitaries U_G (possibly empty) such that $U_G^s = U_F$. Clearly U_G has this property if and only if $G^s = F$. Suppose, for the sake of definiteness, that F is type 1, so that

$$F = S \begin{pmatrix} \theta^r & 0 \\ 0 & (\det F)\theta^{-r} \end{pmatrix} S^{-1} \qquad (167)$$

for some S, r. Then G is an sth root if and only if

$$G = S \begin{pmatrix} \theta^t & 0 \\ 0 & \Delta\theta^{-t} \end{pmatrix} S^{-1} \qquad (168)$$

for some t, Δ such that $st = r$ (mod $d - 1$) and $\Delta^s = \det F$. The problem of finding the roots of a type 2 or 3 matrix is equally straightforward.

6. SIC-POVMs

The results in the last section are potentially relevant to the problem of constructing SIC-POVMs (symmetric informationally complete positive operator valued measures) in prime dimension. Every known [80] SIC-POVM which is covariant under the Weyl-Heisenberg group can be constructed from a fiducial vector which is an eigenvector of a symplectic unitary U_F for which $\mathrm{Tr}(F) = -1$ (mod d). It is therefore of some interest to find a natural basis for the appropriate eigenspace. The results in the last section enable us to do that in every odd prime dimension (since if d is prime the Galoisian variant of the Weyl-Heisenberg Group considered in this paper coincides with the ordinary variant).

Throughout this section it will be assumed without comment that d is prime number ≥ 5 (our analysis does not apply to the case $d = 3$) . If $t = \text{Tr}(F) = -1$ and F is symplectic then $t^2 - 4\Delta = -3$. It is a standard result that $-3 \in Q$ (respectively $-3 \in N$) if $d = 1 \pmod 6$ (respectively $d = 5 \pmod 6$) (see, for example, Hardy and Wright [83]). So F is type 1 if $d = 1 \pmod 6$ and type 2 if $d = 5 \pmod 6$.

Consider first the case $d = 6m + 1 = 1 \pmod 6$. Without loss of generality we can take F to be the matrix

$$F = \begin{pmatrix} \theta^{2m} & 0 \\ 0 & \theta^{-2m} \end{pmatrix} \tag{169}$$

Define

$$G = \begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix} \tag{170}$$

Then $U_F = U_G^{2m}$. U_G is the permutation matrix

$$U_G = -\sum_{r=0}^{d-1} |\theta r\rangle\langle r| \tag{171}$$

Define

$$|\psi_r\rangle = \frac{1}{\sqrt{d-1}} \sum_{s=1}^{d-1} \sigma^{-r \log_\theta s} |s\rangle \tag{172}$$

where $\sigma = e^{\frac{\pi i}{3m}}$ and $r = 0, 1, \ldots, 6m - 1$. Also define

$$|\psi'_0\rangle = |0\rangle \tag{173}$$

Then it is readily confirmed

$$U_G|\psi_r\rangle = \sigma^r |\psi_r\rangle \tag{174}$$

for $r = 0, 1, \ldots, d - 2$, and

$$U_G|\psi'_0\rangle = |\psi'_0\rangle \tag{175}$$

Consequently

$$U_F|\psi_r\rangle = \lambda^r |\psi_r\rangle \tag{176}$$

for $r = 0, 1, \ldots, 6m - 1$ (where $\lambda = e^{\frac{2\pi i}{3}}$), and

$$U_F|\psi'_0\rangle = |\psi'_0\rangle \tag{177}$$

It appears from Scott and Grassl's exhaustive numerical investigation [80] that the fiducial lies in the eigenspace of highest dimension, which is the one with eigenvalue 1 spanned by the $2m + 1$ vectors $|\psi'_0\rangle, |\psi_0\rangle, |\psi_3\rangle, \ldots, |\psi_{6m-3}\rangle$.

Now consider the case $d = 6m - 1 = 5 \pmod 6$. Without loss of generality we can take F to be the matrix

$$F = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \tag{178}$$

(the Zauner matrix [65]). This is a type 2 matrix, and therefore not diagonalizable. However, we can still use the techniques described in the last section to find an order $6m$ symplectic matrix G such that $F = G^{2m}$. It will turn out that the eigenvalues

of the unitary U_G are all non-degenerate, which means that it provides us with a natural basis for the subspace in which the fiducial is hypothesized to lie.

To see this observe

$$F = \begin{pmatrix} 1 & -\frac{\eta^{-4m}}{\eta^{4m}-1} \\ -\eta^{4m} & \frac{\eta^{4m}}{\eta^{4m}-1} \end{pmatrix} \begin{pmatrix} \eta^{4m} & 0 \\ 0 & \eta^{-4m} \end{pmatrix} \begin{pmatrix} 1 & -\frac{\eta^{-4m}}{\eta^{4m}-1} \\ -\eta^{4m} & \frac{\eta^{4m}}{\eta^{4m}-1} \end{pmatrix}^{-1} \tag{179}$$

So if we define

$$G = \begin{pmatrix} 1 & -\frac{\eta^{-4m}}{\eta^{4m}-1} \\ -\eta^{4m} & \frac{\eta^{4m}}{\eta^{4m}-1} \end{pmatrix} \begin{pmatrix} \eta^{2} & 0 \\ 0 & \eta^{-2} \end{pmatrix} \begin{pmatrix} 1 & -\frac{\eta^{-4m}}{\eta^{4m}-1} \\ -\eta^{4m} & \frac{\eta^{4m}}{\eta^{4m}-1} \end{pmatrix}^{-1}$$
$$= \begin{pmatrix} \gamma_{m+1} & -\gamma_1 \\ \gamma_1 & \gamma_{m-1} \end{pmatrix} \tag{180}$$

where

$$\gamma_r = \frac{\eta^{2r} - \eta^{-2r}}{\eta^{2m} - \eta^{-2m}} \tag{181}$$

the matrix G will have the desired property $F = G^{2m}$. Note that we can use the same trick to calculate an arbitrary power of G:

$$G^r = \begin{pmatrix} 1 & -\frac{\eta^{-4m}}{\eta^{4m}-1} \\ -\eta^{4m} & \frac{\eta^{4m}}{\eta^{4m}-1} \end{pmatrix} \begin{pmatrix} \eta^{2r} & 0 \\ 0 & \eta^{-2r} \end{pmatrix} \begin{pmatrix} 1 & -\frac{\eta^{-4m}}{\eta^{4m}-1} \\ -\eta^{4m} & \frac{\eta^{4m}}{\eta^{4m}-1} \end{pmatrix}^{-1}$$
$$= \begin{pmatrix} \gamma_{m+r} & -\gamma_r \\ \gamma_r & \gamma_{m-r} \end{pmatrix} \tag{182}$$

Note also that, for all r,

$$\gamma_r^d = \frac{(\eta^{2r} - \eta^{-2r})^d}{(\eta^{2m} - \eta^{-2m})^d} = \frac{\eta^{2dr} - \eta^{-2dr}}{\eta^{2dm} - \eta^{-2dm}} = \gamma_r \tag{183}$$

(since $\eta^d = -\eta^{-1}$). So even though it is defined in terms of the quantity η, which lies outside the field $\mathbb{F}_d$, γ_r itself lies in the field $\mathbb{F}_d$. Finally, it should be observed that the matrix G is not unique. In fact if k is any integer relatively prime to $d^2 - 1$ then $\bar{\theta}^k$ is also a primitive element of $\mathbb{F}_{d^2}$. So η in the above formulae can be replaced with η^k, for any such k. For the convenience of the reader one possible choice of the matrix G is listed in Table 3 for each of the first 18 primes $= 5 \pmod 6$.

Now consider the unitary U_G. Since U_G is order $d+1$ its eigenvalues are powers of $\sigma = e^{\frac{\pi i}{3m}}$. The projector onto the eigenspace of U_G with eigenvalue σ^r is

$$P_r = \frac{1}{6m} \sum_{s=0}^{6m-1} \sigma^{-rs} U_G^s \tag{184}$$

To find the dimensions of the eigenspaces we need to calculate $\text{Tr}(U_G^s) = \text{Tr}(U_{G^s})$. This can be done using Theorem 5. Let $t_s = \text{Tr}(G^s)$. We have

$$t_s - 2 = \gamma_{m+s} + \gamma_{m-s} = (\eta^s - \eta^{-s})^2 \tag{185}$$

So $t_s = 2$ if and only if $s = 0 \pmod{6m}$. Also

$$(\eta^s - \eta^{-s})^d = \eta^{ds} - \eta^{-ds} = (-1)^{s+1}(\eta^s - \eta^{-s}) \tag{186}$$

d	G	d	G	d	G
5	$\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$	47	$\begin{pmatrix} -12 & -3 \\ 3 & -15 \end{pmatrix}$	101	$\begin{pmatrix} 9 & 42 \\ -42 & -50 \end{pmatrix}$
11	$\begin{pmatrix} -4 & 2 \\ -2 & -2 \end{pmatrix}$	53	$\begin{pmatrix} -22 & 8 \\ -8 & -14 \end{pmatrix}$	107	$\begin{pmatrix} -47 & 31 \\ -31 & -16 \end{pmatrix}$
17	$\begin{pmatrix} 6 & -8 \\ 8 & -2 \end{pmatrix}$	59	$\begin{pmatrix} -25 & 28 \\ -28 & 3 \end{pmatrix}$	113	$\begin{pmatrix} 56 & -47 \\ 47 & 9 \end{pmatrix}$
23	$\begin{pmatrix} 11 & -7 \\ 7 & 4 \end{pmatrix}$	71	$\begin{pmatrix} 8 & 34 \\ -34 & -29 \end{pmatrix}$	131	$\begin{pmatrix} -44 & 11 \\ -11 & -33 \end{pmatrix}$
29	$\begin{pmatrix} 12 & -9 \\ 9 & 3 \end{pmatrix}$	83	$\begin{pmatrix} 18 & -25 \\ 25 & -7 \end{pmatrix}$	137	$\begin{pmatrix} -58 & 20 \\ -20 & -38 \end{pmatrix}$
41	$\begin{pmatrix} 7 & 11 \\ -11 & 18 \end{pmatrix}$	89	$\begin{pmatrix} -25 & -12 \\ 12 & -37 \end{pmatrix}$	149	$\begin{pmatrix} 47 & -12 \\ 12 & 35 \end{pmatrix}$

TABLE 3. One possible choice for the matrix G for each of the first 18 prime dimensions $= 5$ (mod 6). Note that other choices are possible.

(since $\eta^{ds} = (-1)^s \eta^{-s}$). So if $s \neq 0$ (mod $6m$) then $\sqrt{t_s - 2} \in \mathbb{F}_d$ if and only if s is odd. Consequently

$$l(t_s - 2) = (-1)^{s+1} = -\sigma^{3ms} \tag{187}$$

for all $s \neq 0$ (mod $6m$). We also have $\gamma_s = 0$ if and only if $s = 0$ (mod $3m$). So it follows from Theorem 5 that

$$\mathrm{Tr}(U_G^s) = -\sigma^{3ms} \tag{188}$$

if $s \neq 0$ (mod $3m$). It is easily seen that

$$G^{3m} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{189}$$

Taking into account the standard result [83]

$$l(-1) = (-1)^{\frac{d-1}{2}} = -(-1)^m \tag{190}$$

we deduce that Eq. (188) continues to hold when $s = 3m$. Consequently

$$\mathrm{Tr}(P_r) = \frac{1}{6m} \left(d - \sum_{s=1}^{6m-1} \sigma^{(3m-r)s} \right) = 1 - \delta_{r,3m} \tag{191}$$

So the eigenspaces are all one dimensional, with the exception of the eigenspace corresponding to $r = 3m$ which is zero dimensional.

Let $|\psi_r\rangle$ be the normalized eigenvector corresponding to the eigenvalue σ^r (notice that $|\psi_r\rangle$ can be calculated, up to a phase, from the explicit formula we have given

for P_r). We have $U_F|\psi_r\rangle = \lambda^r|\psi_r\rangle$, where $\lambda = \sigma^{2m} = e^{\frac{2\pi i}{3}}$. Let $\mathcal{S}_k$ be the eigenspace of U_F with eigenvalue λ^k. Then bases and dimensions of these subspaces are as in Table 4. Scott and Grassl's exhaustive numerical investigation [80] suggests that fiducial vectors always exist in $\mathcal{S}_1$ and $\mathcal{S}_2$, and that if $m = 0 \pmod 3$ they also exist in $\mathcal{S}_0$.

subspace	basis	dimension
$\mathcal{S}_0$	$|\psi_0\rangle, |\psi_3\rangle, \ldots, |\psi_{3m-3}\rangle, |\psi_{3m+3}\rangle, \ldots, |\psi_{6m-3}\rangle$	$2m-1$
$\mathcal{S}_1$	$|\psi_1\rangle, |\psi_4\rangle, \ldots, |\psi_{6m-2}\rangle$	$2m$
$\mathcal{S}_2$	$|\psi_2\rangle, |\psi_5\rangle, \ldots, |\psi_{6m-1}\rangle$	$2m$

TABLE 4.

7. Representing the F Matrices as Permutation Matrices

The matrices $F \in \mathrm{ESL}(2, \mathbb{F})$ permute the vectors $\mathbf{u} \in (\mathbb{F}_d)^2$ which label the displacement operators. For many purposes it would be convenient if we could label the vectors by an integer r, so that F acts according to the rule $F\colon \mathbf{u}_r \to \mathbf{u}_{f(r)}$ for some function f acting on the index (it will, for instance, be convenient in Section 10). Of course one could assign the integer label arbitrarily. However, one would like to find a natural way of doing it, such that the function f takes a simple form for every $F \in \mathrm{ESL}(2, \mathbb{F}_d)$.

We can achieve this by borrowing an idea from quantum optics. In the analysis of continuous variable systems it is often convenient to replace the two quadratures q, p with the single complex variable

$$\alpha = \frac{1}{\sqrt{2}}(q + ip) \tag{192}$$

One can obtain a discrete analogue of this by letting the extension field $\mathbb{F}_{d^2}$ play the role of $\mathbb{C}$. We accordingly define, for each $\mathbf{u} \in (\mathbb{F}_d)^2$,

$$x(\mathbf{u}) = \eta^{-1} u_1 + u_2 \tag{193}$$

(one is free to use any basis for $\mathbb{F}_{d^2}$ in this definition; we choose the basis $\{\eta^{-1}, 1\}$ because that will prove convenient in Section 10). The map $\mathbf{u} \to x(\mathbf{u})$ is easily seen to be a bijection of $(\mathbb{F}_d)^2$ onto $\mathbb{F}_{d^2}$, with inverse

$$x \to \mathbf{u}(x) = \begin{pmatrix} \frac{x - x^d}{\eta + \eta^{-1}} \\ \frac{\eta x + \eta^{-1} x^d}{\eta + \eta^{-1}} \end{pmatrix} \tag{194}$$

This suggests that we define

$$D_x^{\mathrm{e}} = D_{\mathbf{u}(x)} \tag{195}$$

("e" for "extension field labelling"). We then have

$$D_x^{\mathrm{e}} D_{x'}^{\mathrm{e}} = \tau^{\langle x, x' \rangle} D_{x+x'}^{\mathrm{e}} \tag{196}$$

for all x, $x' \in \mathbb{F}_{d^2}$, where

$$\langle x, x' \rangle = \text{tr} \left(\frac{x^d x' - x x'^d}{\eta + \eta^{-1}} \right) \tag{197}$$

Let us now consider the action of an arbitrary symplectic/anti-symplectic matrix

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{198}$$

It is readily verified that

$$U_F^\dagger D_x^{\text{e}} U_F^\dagger = D_{ax+bx^d}^{\text{e}} \tag{199}$$

for all x, where

$$a = \frac{\eta^{-1}\alpha + \beta + \gamma + \eta\delta}{\eta + \eta^{-1}} \tag{200}$$

$$b = \frac{-\eta^{-1}\alpha + \eta^{-2}\beta - \gamma + \eta^{-1}\delta}{\eta + \eta^{-1}} \tag{201}$$

It is worth examining the map defined by Eqs. (200), (201) in a little more detail. In the first place observe that it is defined for all matrices F (including the singular ones), and not just for the matrices $\in \text{ESL}(2, \mathbb{F}_d)$. Furthermore, it is invertible, with inverse

$$\alpha = \frac{\eta^{-1}(a - b^d) + \eta(a^d - b)}{\eta + \eta^{-1}} \tag{202}$$

$$\beta = \frac{(a - b^d) - (a^d - b)}{\eta + \eta^{-1}} \tag{203}$$

$$\gamma = \frac{(a + \eta^{-2}b^d) - (a^d + \eta^2 b)}{\eta + \eta^{-1}} \tag{204}$$

$$\delta = \frac{\eta(a + \eta^{-2}b^d) + \eta^{-1}(a^d + \eta^2 b)}{\eta + \eta^{-1}} \tag{205}$$

It is thus a bijection of the set of all 2×2 matrices over $\mathbb{F}_d$ onto the set of all pairs $\in (\mathbb{F}_{d^2})^2$. It obviously preserves the additive structure. Moreover, if we equip $(\mathbb{F}_{d^2})^2$ with the product rule

$$(a, b) \circ (a', b') = (aa' + bb'^d, ab' + ba'^d) \tag{206}$$

it also preserves the multiplicative structure (it is a ring isomorphism, in other words). Observe, further, that if F is any 2×2 matrix over $\mathbb{F}_d$, and if (a, b) is the corresponding element of $(\mathbb{F}_d)^2$, then

$$\det F = a^{d+1} - b^{d+1} \tag{207}$$

So we can identify $\text{ESL}(2, \mathbb{F}_d)$ with the set

$$\{(a, b) \in (\mathbb{F}_{d^2})^2 : a^{d+1} - b^{d+1} = \pm 1\} \tag{208}$$

equipped with the above product rule.

We are now ready to address the problem with which we started. For each $0 \leq r \leq d^2 - 2$ define

$$\mathbf{u}_r = \mathbf{u}(\bar{\theta}^{-r}) \tag{209}$$

(we define it like this, with a negative exponent of $\bar{\theta}$, with a view to later convenience). We then have

$$F\mathbf{u}_r = \mathbf{u}_{r-\log_{\bar{\theta}}(a+b\eta^{-2r})} \tag{210}$$

So this gives us a natural way to represent $\mathrm{ESL}(2,\mathbb{F}_d)$ as a group of permutation matrices. Note that the zero vector is excluded from the labelling scheme; however this does not matter because $\mathbf{0}$ is invariant under the action of $\mathrm{ESL}(2,\mathbb{F}_d)$.

Finally observe that if

$$A = \begin{pmatrix} 0 & 1 \\ 1 & \eta - \eta^{-1} \end{pmatrix} \tag{211}$$

then

$$A\mathbf{u}_r = \mathbf{u}_{r-\frac{d-1}{2}} \tag{212}$$

So A is represented by a shift operator. This is a consequence of choosing the basis $\{\eta^{-1}, 1\}$ in Eq. (193). With a different choice of basis for $\mathbb{F}_{d^2}$ one can arrange that any other order $2(d+1)$ anti-symplectic becomes a shift operator.

8. The MUB Cycling Problem: Preliminaries

Wootters and Sussman [25] have shown that if d is a power of 2 there exists a Clifford unitary which cycles through a full set of mutually unbiassed bases (MUBs). In the next two sections we address the problem of generalizing their result to the case when d is an odd prime power dimension.

Let us stress that, throughout the remainder of this paper, we use such phrases as "the full set of MUBs" to mean "the full set of MUBs generated by acting on the standard basis with elements of the group $\mathcal{E}_d^{\mathrm{r}}$" (which, as we will see, is just the set of MUBs orignally described by Wootters and Fields [33]). It is possible to generate other MUBs by acting with the larger group $\mathcal{E}_d$. Also there is, of course, the possibility that there exist full sets of MUBs which are not covariant with respect to any version of the Clifford group.

We will show:

(1) There is no Clifford unitary which cycles through all the MUBs for any d.
(2) If $d = 3 \pmod 4$ there is an anti-Clifford anti-unitary which cycles through all the MUBs.
(3) For every d the MUBs can be divided into 2 groups of $\frac{d+1}{2}$ in such a way that there is a Clifford unitary which cycles through all the MUBs in each group separately.

Let us stress once again that we are confining ourselves to the unitaries/anti-unitaries $\in \mathcal{E}_d^{\mathrm{r}}$. As Gross and Chaturvedi [86] have observed the considerations which follow are not sufficient to exclude the possibility that there exist unitaries or (when $d = 1 \pmod 4$) anti-unitaries $\in \mathcal{E}_d$ which cycle through all the MUBs (except, of course, in prime dimension when the restricted and unrestricted groups are identical).

In a subsequent paper this result will be used to show that minimum uncertainty states [25, 26, 77] exist in every odd prime power dimension, thereby extending Wootters and Sussman's result [25, 26], that such states exist in every even prime power dimension, and in a certain infinite class of dimensions $= 3 \pmod 4$.

The purpose of this section is to fix notation, and to derive a formula which describes how an arbitrary matrix $F \in \mathrm{ESL}(2,\mathbb{F}_d)$ moves us between the different MUBs. In the next section we will prove our main result.

Let

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{213}$$

be any element of $\mathrm{SL}(2, \mathbb{F}_d)$. It can be seen from Eq. (76) that if $\beta = 0$ then U_F simply permutes and re-phases the standard basis. If, on the other hand, $\beta \neq 0$ every element of U_F has modulus $\frac{1}{\sqrt{d}}$. So if we define

$$H_\mu = \begin{cases} \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} & \mu \neq \infty \\ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \mu = \infty \end{cases} \tag{214}$$

and

$$|\mu, x\rangle = U_{H_\mu}|x\rangle \tag{215}$$

and allow μ to vary over the set $\mathbb{F}_d \cup \{\infty\}$, this will give us a full set of $d + 1$ MUBs. The reader will easily perceive that, *modulo* some differences in the phase and labelling conventions, these are the MUBs originally described by Wootters and Fields [33].

Let us now consider the action of the extended Clifford group operators. For the displacement operators we have

$$D_{\mathbf{u}}|\mu, x\rangle = \begin{cases} \tau^{\mathrm{tr}((2x + u_1 - \mu u_2)u_2))}|\mu, x + u_1 - \mu u_2\rangle & \mu \neq \infty \\ \tau^{\mathrm{tr}((2x - u_2)u_1)}|\mu, x - u_2\rangle & \mu = \infty \end{cases} \tag{216}$$

Turning to the case of the symplectic and anti-symplectic operators let

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{217}$$

be any element of $\mathrm{ESL}(2, \mathbb{F}_d)$, and let $\Delta = \det F$. Then

$$FH_\mu = \begin{cases} \begin{pmatrix} 1 & \frac{\alpha\mu + \beta}{\gamma\mu + \delta} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{\Delta}{\gamma\mu + \delta} & 0 \\ \gamma & \gamma\mu + \delta \end{pmatrix} & \mu \neq \infty, \gamma\mu + \delta \neq 0 \\ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -\gamma & 0 \\ \alpha & -\frac{\Delta}{\gamma} \end{pmatrix} & \mu \neq \infty, \gamma\mu + \delta = 0 \\ \begin{pmatrix} 1 & \frac{\alpha}{\gamma} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{\Delta}{\gamma} & 0 \\ -\delta & \gamma \end{pmatrix} & \mu = \infty, \gamma \neq 0 \\ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \delta & 0 \\ -\beta & \alpha \end{pmatrix} & \mu = \infty, \gamma = 0 \end{cases} \tag{218}$$

Consequently

$$
U_F|\mu, x\rangle =
\begin{cases}
l\left(\frac{\Delta}{\gamma\mu+\delta}\right)\tau^{\mathrm{tr}\left(\frac{\Delta\gamma x^2}{\gamma\mu+\delta}\right)}\left|\frac{\alpha\mu+\beta}{\gamma\mu+\delta}, \frac{\Delta x}{\gamma\mu+\delta}\right\rangle & \mu \neq \infty,\ \gamma\mu+\delta \neq 0 \\[2mm]
l\left(-\gamma\right)\tau^{-\mathrm{tr}\left(\alpha\gamma x^2\right)}\left|\infty, -\gamma x\right\rangle & \mu \neq \infty,\ \gamma\mu+\delta = 0 \\[2mm]
l\left(\frac{\Delta}{\gamma}\right)\tau^{-\mathrm{tr}\left(\frac{\Delta\delta x^2}{\gamma}\right)}\left|\frac{\alpha}{\gamma}, \frac{\Delta x}{\gamma}\right\rangle & \mu = \infty,\ \gamma \neq 0 \\[2mm]
l\left(\delta\right)\tau^{-\mathrm{tr}\left(\beta\delta x^2\right)}\left|\infty, \delta x\right\rangle & \mu = \infty,\ \gamma = 0
\end{cases}
\tag{219}
$$

In particular the Wootters-Fields MUBs are the only MUBs which can be got by acting on the standard basis with the unitaries/anti-unitaries $\in \mathcal{E}_d^{\mathrm{r}}$.

9. The MUB Cycling Problem: Main Results

We are now ready to prove our main results. The matrix H_μ is order p if $\mu \neq \infty$, and order 4 if $\mu = \infty$. So if one wants to generate all the MUBs by acting on the standard basis with powers of the operators U_{H_μ} one needs to use a minimum of $p^{n-1}+1$ different operators. We will now show that it is possible to generate them using a much smaller number of operators. Specifically, we will show that in every odd prime power dimension it is possible to generate every MUB by acting on two distinguished bases with powers of a single unitary operator, and that if $d = 3$ (mod 4) one can generate every MUB by acting on any single basis with powers of a single anti-unitary operator.

It can be seen from Eq. (216) that the displacement operators simply permute the vectors within a basis. So if one is interested in finding operators which cycle through the largest possible number of different bases one may confine oneself to the symplectic unitaries and anti-symplectic anti-unitaries.

It follows from Eq. (219) that, for any $F \in \mathrm{ESL}(2, \mathbb{F}_d)$,

$$
U_F|\mu, x\rangle = e^{i\theta_F(\mu, x)}|f_F(\mu), g_F(\mu, x)\rangle
\tag{220}
$$

for suitable functions θ_F, f_F, g_F. We will say that F is a cycling matrix if one gets the complete set of MUBs by acting on any single MUB with powers of U_F.

Let us begin by observing that if F is a cycling matrix, then so is every conjugate of F. In fact suppose that F is cycling, and suppose $F' = SFS^{-1}$ for some $S \in \mathrm{ESL}(2, \mathbb{F}_d)$. The fact that F is cycling means that, for all μ, $f_F^m(\mu) = \mu$ if and only if $m = 0 \pmod{d+1}$. Since $f_F^m(\mu) = \mu$ if and only if $f_F^m(f_S(\mu)) = f_S(\mu)$ it follows that $f_{F'}$ has the same property, implying that F' is also a cycling matrix.

It will be convenient to define the cycling index c_F to the smallest positive integer m such that $f_F^m(0) = 0$. In view of Eq. (76) c_F is the smallest integer m such that F^m is of the form

$$
F^m = \begin{pmatrix} \alpha & 0 \\ \gamma & \delta \end{pmatrix}
\tag{221}
$$

Since c_F divides the order of F, and since the order of every type 1 matrix is $\leq d-1$, we can immediately conclude that no type 1 matrix is a cycling matrix. It is also easily from Tables 1 and 2 together with Eq. (158) that $c_F = 1$ or p for every type 3 matrix. So if cycling matrices exist they have to be type 2. Every type 2 matrix is conjugate to a power of the anti-symplectic matrix

$$
A = \begin{pmatrix} 0 & 1 \\ 1 & \eta - \eta^{-1} \end{pmatrix}
\tag{222}
$$

It is easily seen that if A^r is a cycling matrix then so is A. We conclude that cycling matrices exist if and only if A is a cycling matrix.

To calculate c_A we use the fact

$$A = S \begin{pmatrix} \eta & 0 \\ 0 & -\eta^{-1} \end{pmatrix} S^{-1} \tag{223}$$

where

$$S = \begin{pmatrix} 1 & \frac{1}{\eta+\eta^{-1}} \\ \eta & -\frac{\eta}{\eta+\eta^{-1}} \end{pmatrix} \tag{224}$$

Consequently

$$A^r = S \begin{pmatrix} \eta^r & 0 \\ 0 & (-1)^r \eta^{-r} \end{pmatrix} S^{-1} = \begin{pmatrix} \beta_{r-1} & \beta_r \\ \beta_r & \beta_{r+1} \end{pmatrix} \tag{225}$$

where

$$\beta_r = \frac{\eta^{dr} - \eta^r}{\eta^d - \eta} \tag{226}$$

(where we have used the fact that $\eta^d = -\eta^{-1}$). So c_A is the smallest positive integer m such that

$$\eta^{m(d-1)} = 1 \tag{227}$$

Now $\eta^{m(d-1)} = 1$ if and only if $m(d-1) = 0 \pmod{2(d+1)}$. So c_A is the smallest positive integer m such that

$$m(d-1) = 2k(d+1) \tag{228}$$

for some k.

Suppose that $d = 4u + 1$ for some u. Then Eq. (228) becomes

$$mu = k(2u+1) \tag{229}$$

Since u and $2u + 1$ are relatively prime we conclude that $c_A = \frac{d+1}{2}$. So A is not a cycling matrix.

Suppose, on the other hand, that $d = 4u + 3 \pmod{4}$. Then Eq. (228) becomes

$$m(2u+1) = 4k(u+1) \tag{230}$$

Since $2u + 1$ and $4(u + 1)$ are relatively prime we conclude $c_A = d + 1$. So A is a cycling matrix.

Finally, note that if A is a cycling matrix then A^r is also a cycling matrix if and only if r and $d + 1$ are relatively prime. In particular, the fact that $d + 1$ is even means that even powers of A are never cycling matrices. So there are no symplectic cycling matrices.

We have thus proved

Theorem 7. *Let d be any odd prime power dimension. Then*

(1) *There are no symplectic cycling matrices.*
(2) *If $d = 1 \pmod 4$ there are no anti-symplectic cycling matrices either.*
(3) *If $d = 3 \pmod 4$ an anti-symplectic matrix F is a cycling matrix if and only if $\mathrm{Tr}(F) = \eta^r - \eta^{-r}$ for some r relatively prime to $d + 1$.*

At this point let us stress once again the point we made earlier, that we are only considering the operators in $\mathcal{E}_d^{\mathrm{r}}$. As Gross and Chaturvedi [86] have observed, the above considerations do not exclude the possibility that for some or all values of

d there is a cycling unitary $\in \mathcal{C}_d$; or that for some or all values of $d = 1 \pmod 4$ there is a cycling anti-unitary $\in \mathcal{E}_d$.

We now turn our attention to what, in the absence of a cycling matrix, might be considered the "next best thing": namely, a matrix F with the property that the MUBs split into two groups of $\frac{d+1}{2}$, in such a way that U_F cycles through each group separately. We will refer to such matrices as half-cycling matrices. As with cycling matrices, if F is half-cycling, then so is every conjugate of F.

For given F and μ define $m_F(\mu)$ to be the smallest positive integer m such that $f_F^m(\mu) = \mu$. Clearly F is a half-cycling matrix if and only if $m_F(\mu) = \frac{d+1}{2}$ for all μ.

Since $m_F(\mu)$ is a factor of $\text{ord}(F)$ for all μ no type 1 matrix can be a half-cycling matrix. Since $m_F(0) = 1$ or p for all type 3 matrices no type 3 matrix can be a half-cycling matrix. So, as with cycling matrices, if half-cycling matrices exist at all they must be type 2. It follows that every half-cycling matrix must be conjugate to a power of the matrix A defined in Eq. (222).

To show that A^r is a half-cycling matrix it is enough to show that $m_{A^r}(\mu) = \frac{d+1}{2}$ for more than half the possible values of μ. So in the following we will assume that $\mu \neq \infty$. Observe that if $f_{A^r}^m(\mu) = \mu$ we must have

$$(U_A)^{mr} |\mu, x\rangle = e^{i\theta} |\mu, kx\rangle \tag{231}$$

for some θ, k. Equivalently

$$U_{A_\mu^{mr}} |0, x\rangle = e^{i\theta} |0, kx\rangle \tag{232}$$

where

$$\begin{aligned}
A_\mu^{mr} &= H_\mu^{-1} A^{mr} H_\mu \\
&= \begin{pmatrix} (\beta_{mr-1} - \mu\beta_{mr}) & (-\beta_{mr}\mu^2 + (\beta_{mr-1} - \beta_{mr+1})\mu + \beta_{mr}) \\ \beta_{mr} & (\beta_{mr}\mu + \beta_{mr+1}) \end{pmatrix}
\end{aligned} \tag{233}$$

Referring to Eq. (76) we see that this implies

$$\beta_{mr}\mu^2 - (\beta_{mr-1} - \beta_{mr+1})\mu - \beta_{mr} = 0 \tag{234}$$

This is a quadratic equation in μ with discriminant

$$(\beta_{mr-1} - \beta_{mr+1})^2 + 4\beta_{mr}^2 = (\eta^{mr} - (-1)^{mr}\eta^{-mr})^2 \tag{235}$$

If the equation has solutions in $\mathbb{F}_d$ the discriminant must $\in Q \cup \{0\}$, implying $\eta^{mr} - (-1)^{mr}\eta^{-mr} \in \mathbb{F}_d$. But

$$\left(\eta^{mr} - (-1)^{mr}\eta^{-mr}\right)^d = -\left(\eta^{mr} - (-1)^{mr}\eta^{-mr}\right) \tag{236}$$

which means that $\eta^{mr} - (-1)^{mr}\eta^{-mr} \in \mathbb{F}_d$ if and only if $\eta^{mr} - (-1)^{mr}\eta^{-mr} = 0$. So $f_{A^r}^m(\mu) = \mu$ implies

$$\eta^{2mr} = (-1)^{mr} \tag{237}$$

or

$$mr(d-1) = 0 \pmod{2(d+1)} \tag{238}$$

Suppose, now, that $d = 1 \pmod 4$. Then Eq. (238) reads

$$mr\left(\frac{d-1}{4}\right) = 0 \pmod{\frac{d+1}{2}} \tag{239}$$

Since $\frac{d-1}{4}$ is relatively prime to $\frac{d+1}{2}$ this implies

$$mr = 0 \quad \left(\text{mod } \frac{d+1}{2}\right) \tag{240}$$

We have thus shown that a necessary condition for $f_{A^r}^m(\mu) = \mu$ is that mr is a multiple of $\frac{d+1}{2}$. But it is readily verified that

$$A_\mu^{\frac{k(d+1)}{2}} = \begin{pmatrix} \eta^{\frac{k(d+1)}{2}} & 0 \\ 0 & \eta^{\frac{k(d+1)}{2}} \end{pmatrix} \tag{241}$$

for all μ. So the condition is not only necessary but also sufficient. It follows that, for all $\mu \neq \infty$,

$$m_{A^r}(\mu) = \frac{\frac{d+1}{2}}{\left[r, \frac{d+1}{2}\right]} \tag{242}$$

In particular, A^r is a half-cycling matrix if and only if r is relatively prime to $\frac{d+1}{2}$.

Suppose, on the other hand, that $d = 3 \pmod 4$. Then Eq. (238) reads

$$mr\left(\frac{d-1}{2}\right) = 0 \pmod{d+1} \tag{243}$$

So a necessary condition for $f_{A^r}^m(\mu) = \mu$ is that mr is a multiple of $d+1$. But it is readily verified that

$$A_\mu^{k(d+1)} = \begin{pmatrix} (-1)^k & 0 \\ 0 & (-1)^k \end{pmatrix} \tag{244}$$

irrespective of the value of μ. So the condition is also sufficient. It follows that, for all $\mu \neq \infty$,

$$m_{A^r}(\mu) = \frac{d+1}{[r, d+1]} \tag{245}$$

In particular, A^r is a half-cycling matrix if and only if r is an even integer such that $\frac{r}{2}$ is relatively prime to $\frac{d+1}{2}$.

We have thus proved

Theorem 8. *Let d be any odd prime power dimension. Then*

(a) *A symplectic matrix F is a half-cycling matrix if and only if $\text{Tr}(F) = \eta^{2r} + \eta^{-2r}$ for some integer r relatively prime to $\frac{d+1}{2}$.*

(b) *If $d = 1 \pmod 4$ an anti-symplectic matrix A is half-cycling if and only if $\text{Tr}(F) = \eta^r - \eta^{-r}$ for some odd integer r relatively prime to $d+1$.*

(c) *If $d = 3 \pmod 4$ there are no half-cycling antisymplectic matrices.*

10. Alternative Labelling Scheme

If we label the MUBs in the way we have been doing so far, in terms of the parameter μ, the cycling structure described in the last section is not very obvious. We would like to construct a labelling scheme which makes it more explicit.

This is, in essence, an easy problem to solve: all we have to do is choose an order $2(d+1)$ anti-symplectic A and then label an arbitrary MUB by the number of applications of U_A required to reach it, starting from some distinguished MUB on the same orbit. If $d = 3 \pmod 4$ it becomes easier still: all one has to do is count the number of applications of U_A needed to reach the MUB of interest starting from the standard basis. However, there is a slight complication due to the connection between the MUBs and the displacement operators: each MUB

determines a maximal commuting set of displacement operators and conversely (namely, the set of displacement operators which it diagonalizes). We would like our labelling scheme to make this relationship transparent. To do that we will make use of the labelling of the displacement operators described in Section 7.

It is easily seen that the maximal commuting sets of displacement operators corresponding to the Wootters-Fields MUBs are all of the form

$$\{D_{w\mathbf{u}}\colon w \in \mathbb{F}_d\} \tag{246}$$

for some fixed $\mathbf{u} \neq \mathbf{0}$. In terms of the labelling of the displacement operators described in Section 7 we have

$$w\mathbf{u}_r = \mathbf{u}_{r-(d+1)\log_\theta w} \tag{247}$$

for all non-zero $w \in \mathbb{F}_d$. This suggests replacing the single integer r with a pair of indices s, t, defined so that s (respectively t) is the unique integer in the range $0 \leq s \leq d$ (respectively $0 \leq t \leq d - 2$) such that

$$r = s + t(d+1) \tag{248}$$

(in other words t and s are, respectively, the quotient and remainder of r on division by $d + 1$). In terms of this double index notation we have

$$w\mathbf{u}_{s,t} = \mathbf{u}_{s,t-\log_\theta w} \tag{249}$$

for all non-zero $w \in \mathbb{F}_d$. So the maximal sets of commuting displacement operators corresponding to the Wootters-Fields MUBs are the $d + 1$ sets

$$\mathcal{S}_s = \{D_{\mathbf{u}_{s,t}}\colon 0 \leq t \leq d - 2\} \cup \{D_{\mathbf{0}}\} \tag{250}$$

obtained as s ranges over the interval $0 \leq s \leq d$. Thus, the index s labels the maximal set and the index t labels the individual displacement operators within the set.

We now define, corresponding to each $\mathcal{S}_s$, the d operators

$$P_{s,x} = \frac{1}{d}\left(1 + \sum_{t=0}^{d-2} \omega^{-\operatorname{tr}(\theta^{-t}x)} D_{\mathbf{u}_{s,t}}\right) \tag{251}$$

It is readily confirmed that the $P_{s,x}$ are rank 1 projection operators and, furthermore, that

$$\operatorname{tr}\left(P_{s,x} P_{s',x'}\right) = \begin{cases} \delta_{x,x'} & s = s' \\ \frac{1}{d} & s \neq s' \end{cases} \tag{252}$$

So if we set

$$P_{s,x} = |s,x\rangle_{\text{c}} \,_{\text{c}}\langle s,x| \tag{253}$$

("c" for "cycling") the vectors $|s,x\rangle_{\text{c}}$ will constitute the full set of MUBs, with s labelling the basis and x labelling the individual vector within the basis. Moreover, $\{|s,x\rangle\colon x \in \mathbb{F}_d\}$ is the basis which diagonalizes the displacement operators in $\mathcal{S}_s$.

To find the relation between this labelling scheme and the one used previously observe that, in view of Eq. (216),

$$\langle \mu,y|P_{s,x}|\mu,y\rangle = \frac{1}{d}\left(1 + \sum_{t=0}^{d-2} \omega^{-\operatorname{tr}(\theta^{-t}x)}\langle \mu,y|D_{\mathbf{u}_{s,t}}|\mu,y\rangle\right)$$

$$= \begin{cases} \frac{1}{d} & \mu \neq \mu_s \\ \delta_{y,\lambda_s x} & \mu = \mu_s \end{cases} \tag{254}$$

implying

$$|s,x\rangle_{\mathrm{c}} \doteq |\mu_s, \lambda_s x\rangle \tag{255}$$

where the notation "$\doteq$" means "equals up to a phase", and where

$$\mu_s = \begin{cases} \frac{\eta^s - \eta^{-s}}{\eta^{s+1} + \eta^{-s-1}} & s \neq \frac{d-1}{2} \\ \infty & s = \frac{d-1}{2} \end{cases} \tag{256}$$

$$\lambda_s = \begin{cases} \frac{\eta + \eta^{-1}}{\eta\theta^{-s} + \eta^{-1}\theta^{-ds}} & s \neq \frac{d-1}{2} \\ 1 & s = \frac{d-1}{2} \end{cases} \tag{257}$$

We also have the inverse relation

$$|\mu, x\rangle \doteq |s_\mu, \frac{1}{\lambda_s} x\rangle_{\mathrm{c}} \tag{258}$$

where

$$s_\mu = \begin{cases} \frac{1}{2}\log_\eta\left(\frac{1+\eta^{-1}\mu}{1-\eta\mu}\right) & \mu \neq \infty \\ \frac{d-1}{2} & \mu = \infty \end{cases} \tag{259}$$

In particular $|0, x\rangle_{\mathrm{c}}$ is the standard basis.

To calculate the action of U_F, for arbitrary $F \in \mathrm{ESL}(2, \mathbb{F}_d)$, let $f_F(s)$ be the unique integer in the range $0 \leq f_F(s) \leq d$ and $g_F(s)$ the unique non-zero element of $\mathbb{F}_d$ such that

$$s - \log_{\bar\theta}(a_F - b_F\eta^{-2s}) = f_F(s) + (d+1)\log_\theta(g_F(s)) \tag{260}$$

(so $\log_\theta(g_F(s))$ is the quotient and $f_F(s)$ is the remainder on division by $d+1$). Then

$$F\mathbf{p}_{s,t} = \mathbf{u}_{f_F(s), t + \log_\theta(g_F(s))} \tag{261}$$

In view of Eq. (251) this means

$$U_F P_{s,x} = \frac{1}{d}\left(\sum_{t=0}^{d-2} \omega^{-\operatorname{tr}(\theta^{-t}g_F(s)x)} D_{\mathbf{u}_{f_F(s),t}}\right) \tag{262}$$

implying

$$U_F|s,x\rangle_{\mathrm{c}} \doteq |f_F(s), g_F(s)x\rangle_{\mathrm{c}} \tag{263}$$

Finally, let us consider the action of the operators U_A, U_{A^2}. We have $a_A = \eta$, $b_A = 0$. In view of Eq. (206) this means $a_{A^m} = \eta^m$, $b_{A^m} = 0$ for all m. So

$$U_{A^2}|s,x\rangle_{\mathrm{c}} \doteq \begin{cases} |s+2, \theta^{-1}x\rangle_{\mathrm{c}} & s < d-1 \\ |s+2, x\rangle_{\mathrm{c}} & s = d-1 \text{ or } d \end{cases} \tag{264}$$

(where addition in the first argument is mod $d+1$). We see that, for all d, U_{A^2} cycles through the even-index and odd-index MUBs separately.

Turning to U_A we have

$$U_A|s,x\rangle_{\mathrm{c}} \doteq \begin{cases} |s+\frac{d+3}{2}, \theta^{-1}x\rangle_{\mathrm{c}} & s < \frac{d-1}{2} \\ |s+\frac{d+3}{2}, x\rangle_{\mathrm{c}} & s \geq \frac{d-1}{2} \end{cases} \tag{265}$$

If $d = 1 \pmod 4$ then $\frac{d+3}{2}$ is even, so U_A, like U_{A^2}, cycles through the even-index and odd-index MUBs separately. But if $d = 3 \pmod 4$ then $\frac{d+3}{2}$ is an odd integer relatively prime to $d+1$, so U_A cycles through all the MUBs.

Lastly, let us note that, although A is a cycling matrix when $d = 3 \pmod 4$, it is rather more convenient to use $A^{\frac{d+3}{2}}$ as this increases the index by 1 each time:

$$U_A^{\frac{d+3}{2}} |s, x\rangle_{\mathrm{c}} \doteq \begin{cases} |s + 1, \theta^{-\frac{d+1}{4}} x\rangle_{\mathrm{c}} & s < d \\ |s + 1, \theta^{-\frac{d-3}{4}} x\rangle_{\mathrm{c}} & s = d \end{cases} \tag{266}$$

11. Concluding Remark

In this paper we have confined ourselves to the group $\mathcal{E}_d^{\mathrm{r}}$. It would obviously be interesting to see how far our results extend to the larger group $\mathcal{E}_d$. It would also be interesting to examine the case of even prime power dimension. We hope to address these questions in future publications.

References

[1] D. Gottesman, "Stabilizer Codes and Quantum Error Correction", Thesis, California Institute of Technology (1997). Available online as quant-ph/9705052.
[2] D. Gottesman, *Phys. Rev. A* **57**, 127 (1998).
[3] D. Gottesman, *Chaos, Solitons and Fractals* **10**, 1749 (1999).
[4] M. Neuhauser, *Journal of Lie Theory*, **12**, 15 (2002).
[5] A. Vourdas, *Phys. Rev. A*, **65**, 042321 (2002).
[6] A. Vourdas, *J. Opt. B: Quantum Semiclass. Opt.* **5**, S581 (2003).
[7] J. Dehaene and B. de Moor, *Phys. Rev. A* **68**, 042318 (2003).
[8] M. van den Nest, J. Dehaene and B. de Moor, *Phys. Rev. A* **69**, 022316 (2004).
[9] A. Vourdas, *J. Phys. A* **37**, 3305 (2004).
[10] A. Vourdas, *Rep. Prog. Phys.* **67**, 267 (2004).
[11] K.S. Gibbons, M.J. Hoffman, W.K. Wootters *Phys. Rev. A* **70**, 062101 (2004).
[12] D.M. Appleby, *J. Math. Phys.* **46**, 052107 (2005).
[13] M. van den Nest, J. Dehaene and B. de Moor, *Phys. Rev. A* **71** 022310 (2005).
[14] E. Hostens, J. Dehaene and B. De Moor, *Phys. Rev. A* **71**, 042315 (2005).
[15] M. van den Nest, J. Dehaene and B. de Moor, *Phys. Rev. A* **71**, 062323 (2005).
[16] M. van den Nest, J. Dehaene and B. de Moor, *Phys. Rev. A* **72** 014307 (2005).
[17] D. Gross, "Finite Phase Space Methods in Quantum Information", Diploma Thesis, Potsdam (2005). Available online at http://gross.qipc.org.
[18] E.F. Galvao, *Phys. Rev. A* **71**, 042302 (2005).
[19] J.P. Paz, A.J. Roncaglia and M. Saraceno, *Phys. Rev. A* **72**, 012309 (2005).
[20] A. Vourdas, *J. Math. Phys.* **47**, 092104 (2006).
[21] C. Cormick, E.F. Galvao, D. Gottesman, J.P. Paz and A.O. Pittenger, *Phys. Rev. A* **73**, 012301 (2006).
[22] D. Gross, *J. Math. Phys.* **47**, 122107 (2006).
[23] S.T. Flammia, *J. Phys. A* **39**, 13483 (2006).
[24] A. Vourdas, *J. Phys. A*, **40**, R285 (2007).
[25] W.K. Wootters and D.M. Sussman, arXiv:0704.1277 (2007).
[26] D.M. Sussman, "Minimum-Uncertainty States and Rotational Invariance in Discrete Phase Space", Thesis, Williams College (2007).
[27] D. Gross, *Appl. Phys. B* **86**, 367 (2007).
[28] D.M. Appleby, I. Bengtsson and S. Chaturvedi, *J. Math. Phys.* **49**, 012102 (2008).
[29] M.B. Elliott, B. Eastin and C.M. Caves, *Phys. Rev. A* **77**, 042307 (2008).

[30] M.R. Kibler, *J. Phys. A* **41**, 375302 (2008).

[31] I.D. Ivanović, *J. Phys. A* **14**, 3241 (1981).

[32] W.K. Wootters, *Ann. Phys. (N.Y.)* **176**, 1 (1987).

[33] W.K. Wootters and B.D. Fields, *Ann. Phys. (N.Y.)* **191**, 363 (1989).

[34] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury and F. Vatan, *Algorithmica* **34**, 512 (2002).

[35] J. Lawrence, C. Brukner and A. Zeilinger, *Phys. Rev. A* **65**, 032320 (2002).

[36] S. Chaturvedi, *Phys. Rev. A*, **65**, 044301 (2002).

[37] C. Archer, quant-ph/0312204 (2004).

[38] A.O. Pittenger and M.H. Rubin, *Linear Alg. Appl.* **390**, 255 (2004).

[39] A. Klappenecker and M. Rötteler, *Lecture Notes in Computer Science* **2948**, 137 (2003).

[40] T. Durt, quant-ph/0401046 (2004).

[41] M. Grassl, in *Proceedings ERATO Conference on Quantum Information Science 2004* (Tokyo, 2004). Also available as quant-ph/0406175.

[42] A.B. Klimov, L.L. Sánchez-Soto and H. de Guise, *J. Phys. A* **38**, 2747 (2005).

[43] J.L. Romero, G. Björk, A.B. Klimov and L.L. Sánchez-Soto, *Phys. Rev. A* **72**, 062310 (2005).

[44] M. Planat and H. Rosu, *Eur. Phys. J. D* **36**, 133 (2005).

[45] A. Klappenecker and M. Rötteler, quant-ph/0502031 (2005).

[46] I. Bengtsson and A. Ericsson, *Open Sys. and Information Dyn.* **12**, 187 (2005).

[47] T. Durt, *J. Phys. A* **38**, 5267 (2005).

[48] A.O. Pittenger and M.H. Rubin, *J. Phys. A* **38**, 6005 (2005).

[49] P. Wocjan and T. Beth, *Quantum Inf. Comput.* **5**, 181 (2005).

[50] C. Godsil and A. Roy, quant-ph/0511004 (2005).

[51] W.K. Wootters, *Found. Phys.* **36**, 112 (2006).

[52] M.R. Kibler, *Int. J. Mod. Phys. B* **20**, 1792 (2006).

[53] M.R. Kibler and M. Planat, *Int. J. Mod. Phys. B* **20**, 1802 (2006).

[54] A.B. Klimov, C. Muñoz and J.L. Romero, *J. Phys. A* **39**, 14471 (2006).

[55] A.J. Scott, *J. Phys. A* **39**, 13507 (2006).

[56] A.B. Klimov, J.L. Romero, G. Björk and L.L Sánchez-Soto, *J. Phys. A* **40**, 3987 (2007).

[57] I. Bengtsson, W. Bruzda, A. Ericsson, J.-Å. Larsson, W. Tadej, K. Zyczkowski, *J. Math. Phys.* **48**, 052106 (2007).

[58] S. Brierley, S. Weigert *Phys. Rev. A* **78**, 042312 (2008).

[59] O. Albouy and M.R. Kibbler, *Journal of Russian Laser Research* **28**, 429 (2007).

[60] D.M. Appleby, arXiv:0905.1428 (2009).

[61] M.R. Kibler, *J. Phys. A* **42**, 353001 (2009).

[62] S. Brierley, S. Weigert *Phys. Rev. A* **79**, 052316 (2009).

[63] S. Brierley, S. Weigert and I. Bengtsson, arXiv:0907.4097 (2009).

[64] S.G. Hoggar, *Geom. Dedic.* **69**, 287 (1998).

[65] G. Zauner, "Quantum designs—foundations of a non-commutative theory of designs", thesis (in German), University of Vienna (1999). Available online at http://www.mat.univie.ac.at/˜neum/papers/physpapers.html.

[66] C.M. Caves, "Symmetric Informationally Complete POVMs," UNM Information Physics Group internal report. Available online at http://info.phys.unm.edu/˜caves/reports/reports.html (1999).

[67] C.A. Fuchs and M. Sasaki, *Quant. Inf. Comput.* **3**, 277 (2003).

[68] J.M. Renes, R. Blume-Kohout, A.J. Scott and C.M. Caves, *J. Math. Phys.* **45**, 2171 (2004).

[69] M. Saniga, M. Planat and H. Rosu, *J. Opt. B: Quantum and Semicl. Optics* **6**, L19 (2005).

[70] C.A. Fuchs, *Quantum Inf. Comput.* **4**, 467 (2004).

[71] J. Řeháček, B.-G. Englert and D. Kaszlikowski, *Phys. Rev. A* **70**, 052321 (2004).

[72] A. Klappenecker, M. Rötteler, I. Shparlinski and A. Winterhof, quant-ph/0503239 (2005).

[73] M. Grassl, *Electronic Notes in Discrete Mathematics* **20**, 151 (2005).

[74] S. Colin, J. Corbett, T. Durt and D. Gross, *J. Opt. B: Quantum and Semicl. Optics* **7**, S778 (2005).

[75] I.H. Kim, *Quant. Inf. Comp.* **7**, 730 (2007).

[76] D.M. Appleby, *Opt. Spect.* **103**, 416 (2007).

[77] D.M. Appleby, H.B. Dang and C.A. Fuchs, arXiv:0707.2071 (2007).

[78] M. Khatirinejad, *Journal of Algebraic Combinatorics* **28**, 333 (2008).

[79] I. Bengtsson and H. Granström, *Open Sys. and Information Dyn.* **16**, 145 (2009).

[80] A.J. Scott and M. Grassl, "SIC-POVMs: a New Computer Study", to appear.

[81] D. Gross, private communication.

[82] R. Lidl and H. Niederreiter, *Finite Fields* (2nd edition, Cambridge University Press, Cambridge, 1997).

[83] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers* (5th edition, Cambridge University Press, Cambridge, 1979).

[84] J.E. Humphreys *Amer. Math. Month.* **82**, 21 (1975).

[85] K.E. Gehles, MSc Thesis, University of Andrews (2002).

[86] D. Gross and S. Chaturvedi, private communication.