On SIC-POVMs in prime dimensions

J. Phys. A: Math. Gen. **39** (2006) 13483–13493 doi:10.1088/0305-4470/39/43/007

On SIC-POVMs in prime dimensions

Steven T Flammia

Department of Physics and Astronomy, University of New Mexico, Albuquerque,
NM 87131, USA

E-mail: sflammia@unm.edu

Received 9 June 2006, in final form 4 September 2006
Published 11 October 2006
Online at stacks.iop.org/JPhysA/39/13483

Abstract
The generalized Pauli group and its normalizer, the Clifford group, have a rich mathematical structure which is relevant to the problem of constructing symmetric informationally complete POVMs (SIC-POVMs). To date, almost every known SIC-POVM fiducial vector is an eigenstate of a 'canonical' unitary in the Clifford group. I show that every canonical unitary in prime dimensions $p > 3$ lies in the same conjugacy class of the Clifford group and give a class representative for all such dimensions. It follows that if even one such SIC-POVM fiducial vector is an eigenvector of such a unitary, then all of them are (for a given such dimension). I also conjecture that in *all* dimensions d, the number of conjugacy classes is bounded above by 3 and depends only on d mod 9, and I support this claim with computer computations in all dimensions <48.

PACS numbers: 03.65.−w, 02.10.De

1. Introduction

In the field of quantum information, many diverse applications make frequent use of the notion of *optimal measurement*: optimal quantum state tomography [1], quantum cloning [2, 3], error-free state discrimination [4, 5], certain quantum key distribution protocols [6, 7] and quantum algorithms [8, 9] are but a few examples. Often, the optimal solution to a problem is given by a generalized measurement known as a *positive-operator valued measure*, or POVM [10]. A POVM is a set of positive operators E_i such that the probability of obtaining the ith outcome is given by $\mathrm{Tr}(E_i\rho)$, where ρ is the density operator for the system being measured. A POVM must satisfy the completeness condition, $\sum_i E_i = 1$, which is equivalent to saying the probabilities of the outcomes must sum to unity. In this paper, we deal only with POVMs having a finite number of elements.

If the statistics of a POVM are sufficient to uniquely determine any quantum state with fixed dimension d, the POVM is said to be *informationally complete* (for that particular d). The notion of informational completeness was first discussed in [11], and subsequently in

0305-4470/06/4313483+11$30.00 © 2006 IOP Publishing Ltd Printed in the UK

[12–15], as well as in [16, 17] when applied to just pure states. Informationally complete POVMs have applications to foundational studies where they play a role in the Bayesian formulation of quantum mechanics [18–21], and make particularly nice 'standard quantum measurements' [22]. Since there are $d^2 - 1$ parameters in an unknown density operator, an informationally complete POVM requires at least $d^2 - 1$ independent measurement outcomes; together with the completeness condition this implies that a *minimal* informationally complete POVM is one with exactly d^2 elements [25]. If an informationally complete POVM is to be maximally efficient at determining a state via tomography, then the POVM elements should be proportional to one-dimensional projectors. If this is the case, and in addition the vectors onto which the POVM elements project are evenly spaced in Hilbert space, i.e. the squared inner products are the same for any pair of distinct vectors, then the POVM is said to be *symmetric*. This motivates the definition of a symmetric informationally complete POVM, or SIC-POVM.

Definition 1. *A SIC-POVM $\mathcal{S}$ on a d-dimensional Hilbert space $\mathbb{C}^d$ is a POVM with d^2 elements E_i such that each $E_i \in \mathcal{S}$ is rank one, i.e. $E_i \propto |\psi_i\rangle\langle\psi_i|$ for some $|\psi_i\rangle \in \mathbb{C}^d$, and each pair of distinct normalized vectors satisfies*

$$|\langle\psi_i|\psi_j\rangle|^2 = \frac{1}{d+1}. \tag{1}$$

Thus, a SIC-POVM is a POVM that is informationally complete, minimal and symmetric. (This is actually redundant because minimal and symmetric implies informationally complete.) SIC-POVMs were discovered by Zauner [26] and independently by Renes *et al* [27]. Exact solutions to equation (1) exist in dimensions 2–13, 15 and 19, and numerical examples exist in all dimensions $\leqslant 45$ [26–32]. SIC-POVMs are known in the mathematical literature as equiangular lines, and have been studied for a number of years in the context of frame theory, *t*-designs and spherical codes [33].

A POVM is *group covariant* [34] if there exists a group G of order d^2 with a projective unitary irreducible representation (UIR) on $\mathbb{C}^d$ such that the conjugation action of the projective UIR on the POVM merely permutes the measurement outcome labels. Nearly every SIC-POVM to date has been constructed using group covariance under the group $\mathbb{Z}_d \times \mathbb{Z}_d$ in a manner defined as follows[1]. Fix an orthonormal basis for $\mathbb{C}^d$, and define the operators

$$D_{jk} = \omega^{jk} \sum_{n=0}^{d-1} \omega^{jn} |n \oplus k\rangle\langle n|, \tag{2}$$

where $\omega = \mathrm{e}^{2\pi \mathrm{i}/d}$ is a primitive dth root of unity and $\oplus$ denotes addition mod d. The operators D_{jk} form a projective UIR of $\mathbb{Z}_d \times \mathbb{Z}_d$ and generate the *generalized Pauli group*, or GP group, denoted $GP(d)$. Then construct a SIC-POVM by finding a normalized *fiducial vector*, $|\psi_0\rangle$, such that the set of distinct vectors in $\{D_{jk}|\psi_0\rangle\}_{j,k=0}^{d-1}$ have the same absolute inner product onto the fiducial state. This implies equation (1), and the SIC-POVM is then formed by the set of subnormalized projectors

$$E_{jk} = \frac{1}{d} D_{jk} |\psi_0\rangle\langle\psi_0| D_{jk}^{\dagger}. \tag{3}$$

In this paper, we are interested solely in SIC-POVMs formed via this construction; for the rest of the paper, 'SIC-POVM' and 'fiducial vector' imply GP covariance.

Since the SIC-POVMs we consider are all covariant under the action of $GP(d)$, we can also consider the action of the normalizer of $GP(d)$ in U(d), the so-called *Clifford group*,

[1] In [27], Renes *et al* mention having numerically constructed SIC-POVMs which are group covariant with respect to four other groups, but these constructions appear not to yield SIC-POVMs in every dimension. Also, [29] constructs *analytic* group covariant solutions using other groups in dimensions 6 and 8.

denoted $C(d)$. Given any fiducial vector $|\psi_0\rangle$ and a Clifford group element U, $U|\psi_0\rangle$ is also a fiducial vector. We can extend $C(d)$ to allow anti-unitary operators as well, obtaining the *extended Clifford group*, denoted $EC(d)$. Then given a fixed fiducial vector $|\psi_0\rangle$, every SIC-POVM in that orbit can be written as $U|\psi_0\rangle$ for some $U \in EC(d)$. Since the action of $C(d)$ or $EC(d)$ on the SIC-POVM is a conjugation action, we are really interested in $C(d)/I(d)$ and $EC(d)/I(d)$, where $I(d)$ is the centre of $U(d)$ consisting of all matrices which are just a phase times the identity matrix. We denote these projected groups as $PC(d)$ and $PEC(d)$, respectively.

We now mention a theorem due to Appleby [31] which characterizes the groups $PC(d)$ and $PEC(d)$. Since we are primarily concerned with prime dimensions >3 in this paper, we will state the theorem restricted to this special case. Recall that the group $\mathsf{SL}(2, p)$ is the group of 2×2 matrices defined over the field $\mathbb{Z}_p$ having unit determinant in $\mathbb{Z}_p$. Define $\mathsf{ESL}(2, p)$ to be the group obtained by adding the generator $J = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ to $\mathsf{SL}(2, p)$.

Theorem 1 (Appleby)**.** *Let p be a prime >3. Then $PC(p)$ is isomorphic to $\mathsf{SL}(2, p) \ltimes \mathbb{Z}_p^2$, and $PEC(p)$ is isomorphic to $\mathsf{ESL}(2, p) \ltimes \mathbb{Z}_p^2$.*

Before we can appreciate the significance of this theorem for our purposes, we need one more definition. Define the *Clifford trace* of any element $U \in PEC(p)$ as follows. From theorem 1, there exists an isomorphic image of U in $\mathsf{ESL}(2, p) \ltimes \mathbb{Z}_p^2$ which we can represent as an ordered pair (F, χ), where $F \in \mathsf{ESL}(2, p)$ and $\chi \in \mathbb{Z}_p^2$. The Clifford trace of U, denoted $\mathrm{Tr}_C(U)$, is defined as $\mathrm{Tr}_C(U) = \mathrm{Tr}(F)$, where the trace on the right-hand side is taken over $\mathbb{Z}_p$. Following Appleby [31], we call any U with $\mathrm{Tr}_C(U) = -1 \bmod p$ a *canonical element*, provided it is not the identity (which can only happen when $p = 3$). As an example of such an element that exists in every finite dimension, define the matrix $Z = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$. This matrix, whose importance was first recognized by Zauner [26], will feature prominently in the main result of this paper. (Colin *et al* [35] also discuss an element of $\mathsf{SL}(2, \bar{d})$ that is conjugacy equivalent to Z and mentions its importance to the SIC-POVM problem.)

The following three conjectures relate theorem 1 to SIC-POVMs through the Clifford trace [26, 31]. All three conjectures assert that a SIC-POVM exists in every finite dimension, but they differ in the properties of the fiducial vectors used to generate the SIC-POVM. Since we are primarily interested in the case of prime dimensions ($p > 3$), we state the conjectures specialized to this case and refer the reader to [31] for a discussion of the more general conjectures.

Conjecture 1 (Appleby)**.** *SIC-POVMs exist for every prime dimension, and every SIC-POVM fiducial vector is an eigenvector of a canonical element of $PC(p)$.*

Conjecture 2 (Zauner)**.** *For every prime dimension, there exists a SIC-POVM fiducial vector that is an eigenvector of the unitary operator associated with the matrix Z.*

Conjecture 3 (Appleby)**.** *SIC-POVMs exist for every prime dimension, and every SIC-POVM fiducial vector is an eigenvector of a canonical element of $PC(p)$ that is conjugate to the matrix Z.*

Conjectures 1 and 2 hold for every known SIC-POVM, and in fact a further extension to all dimensions (not just primes) also holds [31]. Conjecture 3 is clearly stronger than conjecture 2, and it also implies conjecture 1. Grassl [29] has constructed a counterexample in dimension 12 to the analogue of conjecture 3 extended to composite dimensions, but there are no known counterexamples in other dimensions. Although conjecture 3 is not true in general, it is important to know for which dimensions it is valid, as the following illustrates.

Because $EC(d)$ acts on $GP(d)$ via conjugation, if one were to search for a SIC-POVM by assuming conjecture 1, it is sufficient to choose one element from each of the conjugacy classes of $EC(d)$ having Clifford trace $= -1$, and search the (degenerate) eigenspaces of these elements. This procedure would yield either a SIC-POVM or (if the search was exhaustive) a counterexample to the conjecture.

The main result of this paper is to show that such a search as described above need only check *one* conjugacy class element if the dimension is a prime >3, thus reducing the search to one over a bounded number of conjugacy classes. This is done by demonstrating the equivalence of all three conjectures when the dimension is prime. This also shows that if one fiducial vector can be found as an eigenvector of the canonical class representative (Z), then every other fiducial vector in prime dimensions >3 automatically satisfies conjecture 1.

Before stating the main result in section 3, we discuss some background results from number theory and prove some theorems applicable to the proof of the main theorem. Readers well versed in number theory may skip section 2 and proceed directly to section 3, although it may be useful to skim the former to glean the notation used in the latter. In section 4, we state an extension of the main theorem and offer supporting numerical evidence.

2. Background results from number theory

In this section we introduce a basic concept from number theory, the Legendre symbol, and state some properties and theorems that will be used in the proof of the main theorem. The basic material can be found in any textbook on the subject (see, for example, [36, 37]), but we review it here for completeness.

Let p be an odd prime and n be any integer such that $\gcd(n, p) = 1$. Then n is a *quadratic residue* mod p if there exists an integer k such that $k^2 = n \bmod p$. If no such integer exists, then n is said to be a *quadratic nonresidue*. Since we will only be dealing with quadratic residues mod p, we will frequently omit the p and the word quadratic and simply say, for example, 'n is a residue', with p and quadratic being understood from the context. We use the symbols $n\ \mathrm{R}p$ and $n\ \mathrm{N}p$ to denote that n is a residue or nonresidue, respectively.

The *Legendre symbol*, $\left(\frac{n}{p}\right)$, is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} +1 & \text{if } n\ \mathrm{R}p, \\ -1 & \text{if } n\ \mathrm{N}p, \\ 0 & \text{if } p|n. \end{cases} \tag{4}$$

Theorem 2. *Let m and n be any integers, and p an odd prime. Then the following properties of the Legendre symbol hold:*

$$\text{Property 1:} \quad \left(\frac{n}{p}\right) = n^{(p-1)/2} \mod p,$$

$$\text{Property 2:} \quad \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right),$$

$$\text{Property 3:} \quad \left(\frac{n^{-1}}{p}\right) = \left(\frac{n}{p}\right),$$

$$\text{Property 4:} \quad \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = 0,$$

$$\text{Property 5:} \quad \left(\frac{-3}{p}\right) = \begin{cases} +1 & \text{if } p = +1 \mod 3, \\ -1 & \text{if } p = -1 \mod 3. \end{cases}$$

Proof. As these properties are very basic, their proofs are not particularly enlightening, so we omit them. See [36, 37] for proofs. Property 1 is known as *Euler's criterion*. Property 4 simply says that the number of residues and nonresidues is exactly $(p-1)/2$. □

We now prove some useful results that we will need in section 3. In the interest of brevity the proofs are concise, but expanded versions of theorems 3 and 4 can be found in [37].

Theorem 3.

$$\sum_{n=1}^{p-2}\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = -1. \tag{5}$$

Proof. Since all integers in the interval $[1, p-2]$ are invertible, we can 'factor' an n out of the second factor in the sum, using property 2 to combine this n with the first factor:

$$\sum_{n=1}^{p-2}\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right) = \sum_{n=1}^{p-2}\left(\frac{n^2}{p}\right)\left(\frac{1+n^{-1}}{p}\right) = \sum_{n=1}^{p-2}\left(\frac{1+n^{-1}}{p}\right). \tag{6}$$

Because all the inverses of elements in the range $[1, p-2]$ are still in that range, this sum has the same value as the following sum, which can be immediately evaluated by reindexing the sum and using property 4:

$$\sum_{n=1}^{p-2}\left(\frac{1+n^{-1}}{p}\right) = \sum_{n=1}^{p-2}\left(\frac{1+n}{p}\right) = -1. \tag{7}$$

□

Theorem 4. *Let $N(p)$ be the number of consecutive residues in the interval* $[1, p-1]$. *Then $N(p)$ is given exactly by*

$$N(p) = \tfrac{1}{4}\left(p - 4 - (-1)^{(p-1)/2}\right). \tag{8}$$

Proof. The proof follows [37]. Let the function $c_p(n)$ be defined by

$$c_p(n) = \begin{cases} 1 & \text{if } n \,\mathrm{R}p \text{ and } (n+1)\,\mathrm{R}p, \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

Thus $c_p(n)$ is the indicator function for adjacent residues. Note that

$$c_p(n) = \frac{1}{4}\left(1+\left(\frac{n}{p}\right)\right)\left(1+\left(\frac{n+1}{p}\right)\right). \tag{10}$$

Then we can write $N(p)$ as

$$N(p) = \sum_{n=1}^{p-2} c_p(n). \tag{11}$$

Expanding the expression for $c_p(n)$, we get four sums:

$$N(p) = \frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)+\left(\frac{n+1}{p}\right)+\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right)\right). \tag{12}$$

The first three can be evaluated using Euler's criterion and property 4, while the last is the content of theorem 3. The result follows directly. □

Theorem 5

$$\sum_{n\,\mathrm{R}p}\left(\frac{n+1}{p}\right) = \frac{(1-p)}{2} + 2N(p) + \frac{1+(-1)^{(p-1)/2}}{2} = -1. \tag{13}$$

Proof. Since there are exactly $(p-1)/2$ residues, the *least* possible value of this sum is achieved if every term is -1, giving the first term in the middle equality. However, this lower bound under counts whenever both n and $n+1$ are residues, so we add $2N(p)$ to correct for this. The only other consideration is if $-1\,\mathrm{R}p$, a term which is not included in the $N(p)$ correction, since 0 is neither a residue nor a nonresidue. In this case, we should add only 1 instead of two, since the Legendre symbol of 0 is 0. The final term

$$\tfrac{1}{2}\left(1+(-1)^{(p-1)/2}\right) \tag{14}$$

has the requisite property. Summing these terms and plugging in the formula from theorem 4 completes the proof. □

Theorem 6. *Let $f(x)$ be a polynomial with integral coefficients. Let $\Upsilon(f)$ be the number of mutually incongruent solutions in x and y to the equation $y^2 = f(x)$ mod p. Then*

$$\Upsilon(f) = p + \sum_{n=0}^{p-1}\left(\frac{f(n)}{p}\right). \tag{15}$$

Proof. If $f(n)\,\mathrm{R}p$, then there are two solutions, $\pm y$. If $f(n)\,\mathrm{N}p$, there are no solutions, and if $f(n) = 0$, there is only one solution, $y = 0$. We simply note that the following term counts the number of solutions correctly for fixed n, and the proof is immediate:

$$\left(1+\left(\frac{f(n)}{p}\right)\right) = \begin{cases} 2 & \text{if } f(n)\,\mathrm{R}p \\ 0 & \text{if } f(n)\,\mathrm{N}p \\ 1 & \text{if } f(n) = 0. \end{cases} \tag{16}$$

□

3. All canonical unitaries are conjugacy equivalent

In this section we prove the main theorem. Throughout this section, assume that p is a prime >3. Because of the isomorphism in theorem 1, we can work exclusively in $\mathsf{ESL}(2,p) \ltimes \mathbb{Z}_p^2$. In fact, we need only work in $\mathsf{SL}(2,p) \ltimes \mathbb{Z}_p^2$ because SIC-POVMs always come in complex conjugate pairs; any fiducial vector which is an eigenvector of an element in $PEC(d)$ that is not an eigenvector of an element of $PC(d)$ will have a conjugate fiducial vector which *is* an eigenvector of an element of $PC(d)$. So a search for a fiducial vector satisfying conjecture 1 need only check elements of $\mathsf{SL}(2,p) \ltimes \mathbb{Z}_p^2$. Recall that the composition rule on $\mathsf{SL}(2,p) \ltimes \mathbb{Z}_p^2$ is defined as follows:

$$(F,\chi)\circ(G,\zeta) = (FG, \chi + F\zeta). \tag{17}$$

The first step is to prove that one need only consider elements of the form $(F, 0)$, which we prove as a separate theorem.

Theorem 7. *For all $(F,\chi) \in \mathsf{SL}(2,p) \ltimes \mathbb{Z}_p^2$ with $\mathrm{Tr}(F) \neq 2$ mod p, (F,χ) is in the same conjugacy class as $(F, 0)$.*

Proof. We would like to show that there always exists $(G,\zeta) \in \mathsf{SL}(2,p) \ltimes \mathbb{Z}_p^2$ such that

$$(G,\zeta)\circ(F,\chi)\circ(G,\zeta)^{-1} = (F,0). \tag{18}$$

To satisfy this conjugacy relation, we will see that it is sufficient to consider elements with $G = I$. Expanding the previous formula with $G = I$, we obtain an equation relating ζ to F and χ:

$$\chi = (F - I)\zeta. \tag{19}$$

This equation can be solved for ζ whenever $\mathrm{Det}(F - I) \neq 0 \bmod p$. Expanding the determinant of $F - I$, we obtain

$$\mathrm{Det}(F) - \mathrm{Tr}(F) + 1 \neq 0, \tag{20}$$

from which the trace condition on F follows immediately. □

The main theorem is concerned with F matrices having trace $= -1 \bmod p$. Since the identity matrix satisfies this condition when $p = 3$, i.e. $\mathrm{Tr}(I) = 2 = -1 \bmod 3$, it is necessary to exclude this case.

Note that in the previous proof, we considered only elements of $\mathsf{SL}(2, p) \ltimes \mathbb{Z}_p^2$ of the form (I, ζ). In the next proof, we work only with $G \in \mathsf{SL}(2, p)$. By concatenating these two results, our general element is of the form (G, ζ).

We now embark on a proof of the main theorem, making use of the results of section 2.

Theorem 8. *Let p be a prime >3, and $F \in \mathsf{SL}(2, p)$ with $\mathrm{Tr}(F) = -1$ mod p. Then there exists a $G \in \mathsf{SL}(2, p)$ such that*

$$GFG^{-1} = Z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}. \tag{21}$$

Proof. Let

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & -1-\alpha \end{pmatrix}, \qquad G = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{22}$$

be matrices in $\mathsf{SL}(2, p)$. Note that the conditions $\mathrm{Det}(F) = -\mathrm{Tr}(F) = 1$ hold, and we have the freedom to choose the matrix elements of G as long as they satisfy the constraint $\mathrm{Det}(G) = 1$. If the matrix elements a and b of G are chosen to be

$$a = c(\alpha + 1) + d\gamma, \qquad b = c\beta - d\alpha, \tag{23}$$

then the relation

$$GF = ZG \tag{24}$$

always holds, so c and d are free parameters that must be chosen to satisfy $\mathrm{Det}(G) = 1$. Expanding the formula for $\mathrm{Det}(G)$ and simplifying, we obtain the following equation for c and d as a function of the matrix elements of F:

$$d^2\gamma + cd(2\alpha + 1) - c^2\beta = 0. \tag{25}$$

We must show that this equation always has a solution, a task which takes up the remainder of the proof. We proceed in three cases: $\gamma = 0$, $\gamma\ \mathrm{R}p$, and $\gamma\ \mathrm{N}p$.

Case 1: $\gamma = 0$

In this case, setting $c = 1$, equation (25) simplifies to

$$d(2\alpha + 1) = \beta. \tag{26}$$

This equation can always be solved for d unless $\alpha = -2^{-1}$. But suppose by contradiction that it was possible that $\alpha = -2^{-1}$. Then comparing with the constraint on the determinant of F, we find that

$$\mathrm{Det}(F) = 1 \mod p \quad \Rightarrow \quad -2^{-1}(-1 + 2^{-1}) = 1 \mod p, \tag{27}$$

which implies that $4 = 1 \bmod p$, something which impossible since $p \neq 3$. This completes the demonstration of case 1.

Before proceeding to the second two cases, it pays to simplify the form of equation (25) using the assumption that $\gamma \neq 0$. Using the fact that $\gcd(2\gamma, p) = 1$, we can complete the square in equation (25) while preserving its solutions to obtain

$$(2\gamma d + c(2\alpha + 1))^2 = (c(2\alpha + 1))^2 + 4\gamma(1 + c^2\beta). \tag{28}$$

Since $4\,\mathrm{R}p$, so is $4^{-1}\,\mathrm{R}p$, and by expanding the right-hand side we can further simplify this to

$$(4^{-1/2}2\gamma d + c4^{-1/2}(2\alpha + 1))^2 = \gamma - 3(4^{-1})c^2. \tag{29}$$

Now a simple change of variables given by

$$x = d\gamma + c(\alpha + 2^{-1}), \qquad y = 2^{-1}c \tag{30}$$

allows this to be written in the very compact form

$$x^2 = \gamma - 3y^2. \tag{31}$$

From this simplified form, we can immediately solve case 2.

Case 2: γ Rp
If $\gamma\,\mathrm{R}p$, simply choose $y = 0$ (implying $c = 0$) and then $x = \gamma^{1/2}$ can be inverted for d. This concludes case 2.

The remaining case is more difficult; it is the reason we developed so much machinery in section 2.

Case 3: γ Np
By theorem 6, the number of solutions Υ to equation (31) is given by

$$\Upsilon = p + \sum_{n=0}^{p-1} \left(\frac{\gamma - 3n^2}{p} \right). \tag{32}$$

By taking out the $n = 0$ term from the sum and 'factoring out' a γ from the Legendre symbol, this becomes

$$\Upsilon = p - 1 - \sum_{n=1}^{p-1} \left(\frac{1 - 3\gamma^{-1}n^2}{p} \right). \tag{33}$$

The sum can now be rewritten to go over only the residues, since n appears only to the second power inside the summand. A factor of two is necessary to account for both the square roots of the residue:

$$\Upsilon = p - 1 - 2 \sum_{n\,\mathrm{R}p} \left(\frac{1 - 3\gamma^{-1}n}{p} \right). \tag{34}$$

This is nearly in a form where theorem 5 is applicable. To get it in such a form, we consider two cases, $p = \pm 1 \bmod 3$, and denote the number of solutions in each case as $\Upsilon_\pm$. First, note that since $\gamma\,\mathrm{N}p$, the sum in equation (34) can be reordered and written as

$$\Upsilon_\pm = p - 1 - 2 \sum_{n\,\mathrm{N}p} \left(\frac{1 - 3n}{p} \right). \tag{35}$$

From property 5 in theorem 2, we know when $-3\,\mathrm{R}p$ or $-3\,\mathrm{N}p$, so equation (35) can be reordered to become

$$\Upsilon_+ = p - 1 - 2 \sum_{n\ \mathrm{N}_p} \left(\frac{n+1}{p}\right), \tag{36}$$

$$\Upsilon_- = p - 1 - 2 \sum_{n\ \mathrm{R}_p} \left(\frac{n+1}{p}\right). \tag{37}$$

To calculate Υ_+, note the following simple identity:

$$\begin{aligned}\sum_{n\ \mathrm{N}_p} \left(\frac{n+1}{p}\right) &= \sum_{n=1}^{p-1} \left(\frac{n+1}{p}\right) - \sum_{n\ \mathrm{R}_p} \left(\frac{n+1}{p}\right) \\ &= -1 - \sum_{n\ \mathrm{R}_p} \left(\frac{n+1}{p}\right),\end{aligned} \tag{38}$$

where property 4 of theorem 2 was used. So the formula for $\Upsilon_\pm$ becomes

$$\Upsilon_\pm = p \pm 1 \pm 2 \sum_{n\ \mathrm{R}_p} \left(\frac{n+1}{p}\right). \tag{39}$$

Now plug in the results of theorem 5 to obtain

$$\Upsilon_\pm = p \mp 1, \tag{40}$$

and so the number of solutions is strictly greater than zero. □

The proof of theorem 8 demonstrates that there is exactly one conjugacy class with trace $= -1 \bmod p$ in the group $\mathsf{SL}(2, p) \ltimes \mathbb{Z}_p^2$ if the dimension p is a prime >3. The consequences for conjectures 1, 2 and 3 are summarized in the following corollary.

Corollary 1. *For prime dimensions $p > 3$, conjectures 1, 2 and 3 are equivalent.*

4. A further conjecture

To state the conjecture, we make use of the extended theorem classifying the Clifford group in non-prime dimensions found in [31]. Let

$$\bar{d} = \begin{cases} d & \text{if } d \text{ is odd,} \\ 2d & \text{if } d \text{ is even.} \end{cases} \tag{41}$$

Then the projective Clifford group $PC(d)$ and the projective extended Clifford group $PEC(d)$ are homomorphic to $\mathsf{SL}(2, \bar{d}) \ltimes \mathbb{Z}_d^2$ and $\mathsf{ESL}(2, \bar{d}) \ltimes \mathbb{Z}_d^2$, respectively. The kernel of the homomorphism is an order 8 subgroup isomorphic to $\mathbb{Z}_2^3$. See [31] for details.

Conjecture 4. *Let T_d denote the number of conjugacy classes of the group $\mathsf{SL}(2, \bar{d})$ (for $d > 1$) having trace $= -1$ mod d. Then T_d is exactly given by*

$$T_d = \begin{cases} 3 & \textit{if } 3|d \textit{ and } 9 \nmid d, \\ 2 & \textit{if } 9|d, \\ 1 & \textit{otherwise.} \end{cases} \tag{42}$$

Note the strange interplay between d and $\bar{d}$. The results of section 3 establish the truth of this conjecture when d is a prime >3. However, the remaining cases are not approachable via a direct application of the methods found here because of the presence of zero divisors in arithmetic modulo d. We therefore leave an analytic demonstration of conjecture 4 to future work, and instead establish its plausibility algorithmically. Using the computer program GAP, we have established the truth of conjecture 4 in all dimensions < 48.

There are two points now worth emphasizing. Conjecture 4 attempts to classify exactly for which dimensions the equivalence of the three conjectures 1, 2 and 3 holds. The answer appears to be ‘any dimension not divisible by 3’. Note that this agrees with the results in [29]. Second, the computer program GAP does *not* use floating-point arithmetic. This means that the algorithmic verification of conjecture 4 in dimensions <48 is *exact*.

5. Conclusion

We have established that all canonical unitaries in the projective Clifford group in a prime dimension >3 lie in the same conjugacy class. Thus, if even one SIC-POVM fiducial vector is an eigenvector of such a unitary, then all of them are (for a given such dimension). We have also advanced a conjecture which would extend this result to all dimensions and offered computer calculations as evidence supporting it in all dimensions <48. These results begin to classify for which dimensions conjectures 1, 2 and 3 are equivalent.

Acknowledgments

Thanks to Andrew Landahl and Seth Merkel for helpful discussions, and to Carl Caves for comments on this manuscript. Markus Grassl also provided valuable suggestions for improving this paper. This research was supported by Office of Naval Research Contract No N00014-03-1-0426.

Note added in proof. After this paper was accepted for publication, a proof of conjecture 4 was discovered to have been proven in references [23] and [24].

References

[1] Paris M and Řeháček J (ed) 2004 *Quantum State Estimation (Lecture Notes in Physics* vol 649*)* (Berlin: Springer)
[2] Gisin N and Massar S 1997 *Phys. Rev. Lett.* **79** 2153
[3] Scott A J 2006 Tight informationally complete quantum measurements *Preprint* quant-ph/0604049
[4] Chefles A 1998 *Phys. Lett.* A **239** 339
[5] Chefles A and Barnett S 1998 *Phys. Lett.* A **250** 223
[6] Renes J M 2004 *Phys. Rev.* A **70** 052314
[7] Renes J M 2005 *Quant. Inf. Comp.* **5** 080
[8] Bacon D, Childs A M and van Dam W 2005 Optimal measurements for the dihedral hidden subgroup problem *Preprint* quant-ph/0501044
[9] Bacon D, Childs A M and van Dam W 2005 *FOCS 2005: Proc. 46th IEEE Symp. on Foundations of Computer Science* pp 469–78
[10] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[11] Prugovečki E 1977 *Int. J. Theor. Phys.* **16** 321
[12] Busch P and Lahti P J 1989 *Found. Phys.* **19** 633
[13] Busch P 1991 *Int. J. Theor. Phys.* **30** 1217
[14] Hellwig K-E 1993 *Int. J. Theor. Phys.* **32** 2401
[15] Peres A 1993 *Quantum Theory: Concepts and Methods* (Dordrecht: Kluwer) (POVMs are discussed in sections 9-5 and 9-6)
[16] Flammia S T, Silberfarb A and Caves C M 2005 *Found. Phys.* **35** 1985
[17] Finkelstein J 2004 *Phys. Rev.* A **70** 052107
[18] Caves C M, Fuchs C A and Schack R 2002 *Phys. Rev.* A **65** 022305
[19] Caves C M, Fuchs C A and Schack R 2002 *J. Math. Phys.* **43** 4537

[20] Fuchs C A and Sasaki M 2003 *Quant. Inf. Comp.* **3** 377

[21] Fuchs C A 2002 *Preprint* quant-ph/0205039

[22] Hardy L 2001 *Preprint* quant-ph/0101012

[23] Nobs A 1976 *Comment. Math. Helv.* **51** (4) 465–89 (German)

[24] Nobs A and Wolfart J 1976 *Comment. Math. Helv.* **51** (4) 491–526 (German)

[25] Weigert S 2006 Simple minimal informationally complete measurements for qudits *Int. J. Mod. Phys.* B **20** 11–13 1942

[26] Zauner G 1999 Quantendesigns—Grundzüge einer nichtkommutativen Designtheorie *PhD Thesis* University of Vienna

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

[28] Grassl M 2004 *Proc. of the ERATO Conf. on Quantum Information Science (Tokyo, Sept.)* p 60

[29] Grassl M 2005 *Electron. Notes Discrete Math.* **20** 151

[30] Grassl M 2006 Private communication

[31] Appleby D M 2005 *J. Math. Phys.* **46** 052107

[32] Hoggar S G 1998 *Geom. Dedic.* **69** 287

[33] Delsarte P, Goethals J M and Seidel J J 1977 *Geom. Dedic.* **6** 363

[34] D'Ariano G M, Perinotti P and Sacchi M F 2004 *J. Opt.* B **6** S487

[35] Colin S, Corbett J, Durt T and Gross D 2005 *J. Opt.* B **7** S778

[36] Kumanduri R and Romero C 1998 *Number Theory with Computer Applications* (Englewood Cliffs, NJ: Prentice-Hall)

[37] Andrews G 1994 *Number Theory* (New York: Dover)