Projective ring line of an arbitrary single qudit

Hans Havlicek[1] **and Metod Saniga**[2]

[1] Institut für Diskrete Mathematik und Geometrie, Technische Universität Wien,
Wiedner Hauptstrasse 8-10, A-1040 Vienna, Austria
[2] Astronomical Institute, Slovak Academy of Sciences, SK-05960 Tatranská Lomnica,
Slovak Republic

E-mail: havlicek@geometrie.tuwien.ac.at and msaniga@astro.sk

Abstract

As a continuation of our previous work (Havlicek and Saniga 2007 *J. Phys. A: Math. Gen.* **40** F943–52 (*Preprint* 0708.4333)) an algebraic geometrical study of a single d-dimensional qudit is made, with d being *any* positive integer. The study is based on an intricate relation between the symplectic module of the generalized Pauli group of the qudit and the fine structure of the projective line over the (modular) ring $\mathbb{Z}_d$. Explicit formulae are given for both the number of generalized Pauli operators commuting with a given one and the number of points of the projective line containing the corresponding vector of $\mathbb{Z}_d^2$. We find, remarkably, that a perp-set is not a set-theoretic union of the corresponding points of the associated projective line unless d is a product of distinct primes. The operators are also seen to be structured into disjoint 'layers' according to the degree of their representing vectors. A brief comparison with some multiple-qudit cases is made.

PACS numbers: 03.65.−a, 03.65.Fd, 02.10.Hh, 02.40.Dr

1. Introduction

In our recent paper [1], we introduced a general algebraic geometrical framework underlying the structure of the generalized Pauli group associated with a specific single d-dimensional qudit. The backbone of this framework is the bijection between sets of operators/matrices of the group and vectors over the modular ring $\mathbb{Z}_d$. This bijection enabled us, for d being a product of distinct primes, to completely rephrase the group's commutation algebra in terms of the structure of and interplay between free cyclic submodules of $\mathbb{Z}_d^2$, also known as points of the projective line defined over $\mathbb{Z}_d$. In this paper we shall tackle the general case (i.e. d being any positive integer), thus making the treatment of a *single* qudit complete.

2. Single *d*-qudit, its qeneralized Pauli group, symplectic module and projective ring line

In this section, we simply set up the notation and recollect some basic technical results from our previous paper [1] to be needed in the following.

Let $d > 1$ be an integer and $\mathbb{Z}_d := \{0, 1, \ldots, d - 1\}$. Addition and multiplication of elements from $\mathbb{Z}_d$ will always be understood modulo d. We consider the d-dimensional complex Hilbert space $\mathbb{C}^d$ and denote by

$$\{|s\rangle : s \in \mathbb{Z}_d\}$$

a computational basis of $\mathbb{C}^d$. A qudit in $\mathbb{C}^d$ is a vector

$$|\psi\rangle = \sum_{s=0}^{d-1} \alpha_s |s\rangle, \qquad \text{where} \qquad \alpha_s \in \mathbb{C} \qquad \text{and} \qquad \sum_{s=0}^{d-1} |\alpha_s|^2 = 1.$$

Taking ω to be a fixed primitive dth root of unity (e.g., $\omega = \exp(2\pi i/d)$), we define unitary X ('shift') and Z ('clock') operators on $\mathbb{C}^d$ via $X|s\rangle = |s + 1\rangle$ and $Z|s\rangle = \omega^s |s\rangle$, respectively, for all $s \in \mathbb{Z}_d$. With respect to our computational basis, the matrices of X and Z are

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & \omega & 0 & \ldots & 0 \\ 0 & 0 & \omega^2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \omega^{d-1} \end{pmatrix},$$

respectively. The (generalized) *Pauli group* generated by X and Z will be denoted as G. For all $s \in \mathbb{Z}_d$, we have $XZ|s\rangle = \omega^s |s + 1\rangle$ and $ZX|s\rangle = \omega^{s+1} |s + 1\rangle$. This gives the basic relation

$$\omega XZ = ZX, \tag{1}$$

which implies that each element of G can be written in the unique *normal form*

$$\omega^a X^b Z^c \quad \text{for some integers} \quad a, b, c \in \mathbb{Z}_d. \tag{2}$$

From (1), it is readily seen that

$$(\omega^a X^b Z^c)(\omega^{a'} X^{b'} Z^{c'}) = \omega^{b'c+a+a'} X^{b+b'} Z^{c+c'},$$

which shows that G is a non-commutative group of order d^3. Next, the *commutator* of two operators W and W' is

$$[W, W'] := WW'W^{-1}W'^{-1}, \tag{3}$$

which in our case acquires the form

$$[\omega^a X^b Z^c, \omega^{a'} X^{b'} Z^{c'}] = \omega^{cb'-c'b} I.$$

Recall that two operators commute if and only if their commutator (taken in any order) is equal to I (the identity matrix).

There are two important normal subgroups of G: its *centre* $Z(G)$ and its *commutator subgroup* G', the two being identical

$$G' = Z(G) = \{\omega^a I : a \in \mathbb{Z}_d\}. \tag{4}$$

The bijective mappings

$$\psi : \mathbb{Z}_d \to G' : a \mapsto \omega^a I,$$
$$\phi : \mathbb{Z}_d^2 \to G/G' : (b, c) \mapsto G' X^b Z^c$$

and their inverses yield a mapping[3]

$$[\cdot, \cdot] : \mathbb{Z}_d^2 \to \mathbb{Z}_d : ((b, c), (b', c')) \mapsto cb' - c'b, \tag{5}$$

which just describes the commutator of two elements of G (given in normal form) in terms of our $\mathbb{Z}_d$-module. The mapping (5) can be rewritten in the following convenient form:

$$[(b, c), (b', c')] = (b, c) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b' \\ c' \end{pmatrix} = \det \begin{pmatrix} b' & c' \\ b' & c' \end{pmatrix}, \tag{6}$$

which implies that $[\cdot, \cdot]$ is a bilinear alternating form on $\mathbb{Z}_d^2$. As usual, we write $(b, c) \perp (b', c')$ if $[(b, c), (b', c')] = 0$ and speak of *orthogonal* (or *perpendicular*) vectors (with respect to $[\cdot, \cdot]$). As our alternating bilinear form is non-degenerate, we have indeed a *symplectic module*.

The set of operators in G which commute with a fixed operator $\omega^a X^b Z^c$ corresponds to the *perpendicular set* (shortly the *perp-set*) of (b, c), namely

$$(b, c)^\perp := \left\{ (u, v) \in \mathbb{Z}_d^2 : (b, c) \perp (u, v) \right\}.$$

Being closed under addition and multiplication by ring elements and fulfilling the condition

$$\mathbb{Z}_d(b, c) \subset (b, c)^\perp,$$

the set $(b, c)^\perp$ is a $\mathbb{Z}_d$-submodule of $\mathbb{Z}_d^2$.

A full algebraic geometrical meaning of perp-sets in $\mathbb{Z}_d^2$ is revealed after introducing the concept of the projective line over the ring $\mathbb{Z}_d$. We sketch here only some basic notions and results, referring the interested reader to [2]–[6] for further details and proofs.

Let us consider any vector $(b, c) \in \mathbb{Z}_d^2$. It generates the cyclic submodule

$$\mathbb{Z}_d(b, c) = \{(ub, uc) : u \in \mathbb{Z}_d\}.$$

Such a cyclic submodule is called *free* if the mapping $u \mapsto (ub, uc)$ is injective. In this case, the vector (or pair) (b, c) is called *admissible*. Any free cyclic submodule of $\mathbb{Z}_d^2$ has precisely d vectors, including the zero vector. However, not all vectors $\neq (0, 0)$ of a free cyclic submodule need to be admissible. In a more geometric language, a free cyclic submodule of $\mathbb{Z}_d^2$ is called a *point*. The point set

$$\mathbb{P}_1(\mathbb{Z}_d) := \{\mathbb{Z}_d(c, d) : (c, d) \text{ is admissible}\}$$

is the *projective line* over the ring $\mathbb{Z}_d$. According to this definition, a point is a set of vectors.

3. A qudit for d a prime power

The case of d being a product of distinct primes was dealt with in [1] where the interested reader can find all the details; following the strategy and employing the findings of this paper, we are now in position to successfully tackle the most general case.

In this section, as a necessary intermediate step, we focus our attention to the case of a single qudit for $d = p^\varepsilon$, where p is a prime and $\varepsilon \geqslant 1$ an integer. Even though we aim at using representatives from $\mathbb{Z}_d$ rather than arbitrary integers (to be reduced modulo d), it will also be very convenient to represent $0 \in \mathbb{Z}_d$ by $d = p^\varepsilon \notin \mathbb{Z}_d$. We remind the reader that exponents in terms such as p^α or $p^{\alpha+\beta}$ are non-negative integers which *must not* be reduced modulo d. Of course, when speaking about cardinalities of sets, also no reduction modulo d has to be applied.

Each of the sets

$$\mathbb{Z}_d = \mathbb{Z}_d \cdot p^0 \supset \mathbb{Z}_d \cdot p^1 \supset \cdots \supset \mathbb{Z}_d \cdot p^\varepsilon = \{0\}$$

---

[3] Of course, the symbol $[\cdot, \cdot]$ has two different meanings in (3) and (5) respectively.

is an ideal of the ring $(\mathbb{Z}_d, +, \cdot)$. We infer from

$$\mathbb{Z}_d \cdot p^\kappa = \{wp^\kappa : w = 1, 2, \ldots, p^{\varepsilon-\kappa}\}$$

that $|\mathbb{Z}_d \cdot p^\kappa| = p^{\varepsilon-\kappa}$ for any $\kappa \in \{0, 1, \ldots, \varepsilon\}$.

An element of $\mathbb{Z}_d$ has a multiplicative inverse if and only if it belongs to $\mathbb{Z}_d \setminus \mathbb{Z}_d \cdot p$. So the elements of $\mathbb{Z}_d$ without an inverse (i.e. the zero divisors of $\mathbb{Z}_d$) are precisely the $p^{\varepsilon-1}$ elements of $\mathbb{Z}_d \cdot p$. We note in passing that $\mathbb{Z}_d \cdot p$ is the only maximal ideal of the ring $\mathbb{Z}_d$. So $\mathbb{Z}_d$ is a *local ring*.

Each element $a \in \mathbb{Z}_d$ admits a factorization of the form

$$a = up^\alpha \qquad \text{with} \quad u \in \mathbb{Z}_d \setminus \mathbb{Z}_d \cdot p \qquad \text{and} \qquad \alpha \in \{0, 1, \ldots, \varepsilon\}. \quad (7)$$

Indeed, $a = 0$ can be written as $a = 1p^\varepsilon$, for $a = 1$ holds $a = 1p^0$, and for any other element of $\mathbb{Z}_d$ the usual decomposition of a into a product of primes, which uses the arithmetics over $\mathbb{Z}$, also gives a solution in $\mathbb{Z}_d$. The integer α is determined uniquely: it is the smallest element $\kappa \in \{0, 1, \ldots, \varepsilon\}$ such that $a \in \mathbb{Z}_d \cdot p^\kappa$. This uniqueness need not hold for u. In the case $a = 0$, the element u may be any invertible element of $\mathbb{Z}_d$. For any $a \neq 0$, the element u is given up to an additive constant belonging to

$$\mathbb{Z}_d \cdot p^{\varepsilon-\alpha} = \{wp^{\varepsilon-\alpha} : w = 1, 2, \ldots, p^\alpha\}.$$

This set is the *annihilator* of p^α, i. e. the set of all $x \in \mathbb{Z}_d$ with the property $p^\alpha x = 0$.

Let (b, c) be a vector of the $\mathbb{Z}_d$-module $\mathbb{Z}_d^2$, where $b = vp^\beta$ and $c = wp^\gamma$ are factorizations as in (7). Then $\min\{\beta, \gamma\}$ will be called the *degree* of (b, c). So this degree equals the smallest index $\kappa \in \{0, 1, \ldots, \varepsilon\}$ such that $b, c \in \mathbb{Z}_d \cdot p^\kappa$. It is an easy exercise to show that (b, c) has degree κ if and only if the ideal of $\mathbb{Z}_d$ generated by $\{b, c\}$ equals $\mathbb{Z}_d \cdot p^\kappa$.

Lemma 1. *Let (b, c) be a vector of $\mathbb{Z}_d^2$ with degree δ. Then the following assertions hold.*

(a) If A is an invertible 2×2 matrix over $\mathbb{Z}_d$ or, in symbols $A \in GL_2(\mathbb{Z}_d)$, then $(b, c)A$ is also a vector of degree δ.

(b) There exists a matrix $M \in GL_2(\mathbb{Z}_d)$ such that $(b, c)M = (p^\delta, 0)$.

Proof. Suppose that $b = vp^\beta$ and $c = wp^\gamma$ are factorized according to (7). Given a matrix $A = (a_{jk}) \in GL_2(\mathbb{Z}_d)$, we obtain from

$$(b, c)A = p^\delta(va_{11}p^{\beta-\delta} + wa_{21}p^{\gamma-\delta}, va_{12}p^{\beta-\delta} + wa_{22}p^{\gamma-\delta})$$

that the degree of $(b, c)A$ is $\geqslant \delta$. Similarly, $((b, c)A)A^{-1} = (b, c)$ implies that the degree of $(b, c)A$ is $\leqslant \delta$. This completes the proof of (a).

In order to establish (b), we distinguish two cases. If $\delta = \beta \leqslant \gamma$, we then put

$$M := \begin{pmatrix} v^{-1} & -wp^{\gamma-\beta} \\ 0 & v \end{pmatrix},$$

whereas for $\delta = \gamma \leqslant \beta$ we put

$$M := \begin{pmatrix} 0 & -w \\ w^{-1} & vp^{\beta-\gamma} \end{pmatrix}.$$

In either case we have $\det M = 1$ and $(b, c)M = (p^\delta, 0)$, as required. $\square$

We add for the sake of completeness that M^{-1} equals

$$\begin{pmatrix} v & wp^{\gamma-\beta} \\ 0 & v^{-1} \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} vp^{\beta-\gamma} & w \\ -w^{-1} & 0 \end{pmatrix},$$

respectively.

Also, we emphasize the particular case of a vector (b, c) with degree 0 or, said differently, of an admissible vector. Such a vector can be moved to $(1, 0)$ by an appropriate invertible matrix. This reflects the well-known fact that all points of the projective line $\mathbb{P}_1(\mathbb{Z}_d)$ form an orbit under the action of the group $GL_2(\mathbb{Z}_d)$.

Lemma 2. *The symplectic form* $[\cdot, \cdot]$ *remains invariant, to within invertible elements of* $\mathbb{Z}_d$, *under the natural action of the general linear group* $GL_2(\mathbb{Z}_d)$ *on* $\mathbb{Z}_d^2$.

Proof. From (6) it follows for all $A \in GL_2(\mathbb{Z}_d)$ and all $(b, c), (b', c') \in \mathbb{Z}_d^2$ that

$$[(b, c)A, (b', c')A] = \det A[(b, c), (b', c')].$$

$\square$

This implies, in particular, that our (symplectic) orthogonality of vectors is preserved under the natural action of $GL_2(\mathbb{Z}_d)$. We shall use lemmas 1 and 2 in the subsequent proofs in order to simplify some (otherwise lengthy) calculations.

Theorem 1. *Let the integer* $d = p^\varepsilon > 1$ *be a power of a prime p. Also, let* (b, c) *be a vector of* $\mathbb{Z}_d^2$ *with degree* δ. *Then the number of points of the projective line* $\mathbb{P}_1(\mathbb{Z}_d)$ *which contain the vector* (b, c) *equals*

$$
\begin{aligned}
&p^\varepsilon + p^{\varepsilon-1} && \text{if} \quad \delta = \varepsilon, \\
&p^\delta && \text{if} \quad \delta < \varepsilon.
\end{aligned}
$$

Proof. Due to lemmas 1 and 2, we may confine ourselves to the case $(b, c) = (p^\delta, 0)$. Each point of $\mathbb{P}_1(\mathbb{Z}_d)$ can be written in a unique way either as $\mathbb{Z}_d(1, y)$, where $y \in \mathbb{Z}_d$ is arbitrary, or as $\mathbb{Z}_d(x, 1)$, with $x \in \mathbb{Z}_d \cdot p$ (see, e.g., [5, page 792]). We distinguish two cases, as follows.

Case 1. We have $(p^\delta, 0) \in \mathbb{Z}_d(1, y)$ if and only if $p^\delta y = 0$, which in turn is equivalent to saying that $y \in \mathbb{Z}_d$ is in the annihilator of p^δ, namely y is one of the elements

$$tp^{\varepsilon-\delta} \in \mathbb{Z}_d \qquad \text{with} \qquad t \in \{1, 2, \dots, p^\delta\}. \tag{8}$$

These elements give rise to p^δ mutually distinct points containing the vector $(p^\delta, 0)$.

Case 2. A point of the form $\mathbb{Z}_d(x, 1)$ contains the vector $(p^\delta, 0)$ precisely when $(p^\delta, 0) = 0(x, 1) = (0, 0)$. Hence for $\delta < \varepsilon$ no such points exist, whereas for $\delta = \varepsilon$ there are $p^{\varepsilon-1}$ points of this kind. $\square$

Our next aim is to count the number of vectors in the perp-set of a vector (b, c).

Theorem 2. *Let the integer* $d = p^\varepsilon > 1$ *be a power of a prime p. Also, let* (b, c) *be a vector of* $\mathbb{Z}_d^2$ *with degree* δ. *Then*

$$|(b, c)^\perp| = p^{\varepsilon+\delta}.$$

Proof. Again, we may assume without loss of generality that $(b, c) = (p^\delta, 0)$. An unknown vector $(x, y) \in \mathbb{Z}_d^2$ belongs to $(p^\delta, 0)^\perp$ if and only if

$$\det \begin{pmatrix} p^\delta & 0 \\ x & y \end{pmatrix} = p^\delta \det \begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix} = 0.$$

By expanding this determinant, we deduce the equivalent condition

$$y \in \{tp^{\varepsilon-\delta} : t = 1, 2, \dots, p^\delta\} \tag{9}$$

in which the unknown x does not appear. So there are precisely p^ε solutions for x and precisely p^δ solutions for y. $\square$

Let us compare the results from theorems 1 and 2. For the sake of completeness, the following result includes some previous findings.

Theorem 3. *Let the integer $d = p^\varepsilon > 1$ be a power of a prime p. Also, let (b, c) be a vector of $\mathbb{Z}_d^2$ with degree δ. We denote by $U(b, c) \subset \mathbb{Z}_d^2$ the set-theoretic union of all points of the projective line $\mathbb{P}_1(\mathbb{Z}_d)$ containing the vector (b, c). Then $U(b, c)$ is a generating set for the submodule $(b, c)^\perp \subset \mathbb{Z}_d^2$. Furthermore, the equality*

$$U(b, c) = (b, c)^\perp \tag{10}$$

holds if and only if one of the following conditions is satisfied:

(a) $(b, c) = (0, 0)$.
(b) (b, c) is an admissible pair.

Proof. The assertions hold trivially for $(b, c) = (0, 0)$, and we rule out this case for the rest of the proof. As before, it will be assumed that $(b, c) = (p^\delta, 0)$ is satisfied. We infer from (9) that $(p^\delta, 0)^\perp$ equals the set of vectors of the form

$$(s, tp^{\varepsilon-\delta}) \qquad \text{with} \quad s \in \mathbb{Z}_d \qquad \text{and} \qquad t \in \{1, 2, \ldots, p^\delta\}. \tag{11}$$

By (8), a vector is in $U(p^\delta, 0)$ if and only if it can be written as

$$(\tilde{s}, \tilde{s}\tilde{t}p^{\varepsilon-\delta}) \qquad \text{with} \quad \tilde{s} \in \mathbb{Z}_d \qquad \text{and} \qquad \tilde{t} \in \{1, 2, \ldots, p^\delta\}. \tag{12}$$

We have $U(p^\delta, 0) \subset (p^\delta, 0)^\perp$, since any vector from (12) also appears in (11) for $s := \tilde{s}$ and the unique element $t \in \{1, 2, \ldots, p^\delta\}$ which satisfies $t \equiv \tilde{s}\tilde{t} \pmod{p^\delta}$. Conversely, each vector of $(p^\delta, 0)^\perp$ is a linear combination of vectors of $U(p^\delta, 0)$, because

$$(s, tp^{\varepsilon-\delta}) = (s - t)(1, 0) + t(1, p^{\varepsilon-\delta}),$$

where we use on the right-hand side those vectors which arise in (12) for $(\tilde{s}, \tilde{t}) := (1, p^\delta)$ and $(\tilde{s}, \tilde{t}) := (1, 1)$. Thus, $U(p^\delta, 0)$ generates $(p^\delta, 0)^\perp$.

We infer from theorem 2 that equation (10) is satisfied precisely when $|U(p^\delta, 0)| = p^{\varepsilon+\delta}$. This in turn is true if and only if distinct pairs $(\tilde{s}, \tilde{t})$ determine distinct vectors in (12). Clearly, distinct values for $\tilde{s}$ yield distinct vectors, but for a fixed $\tilde{s}$ and a variable $\tilde{t}$ this need no longer be true. Indeed, let us fix some $\tilde{s} \in \mathbb{Z}_d$. Furthermore, we assume that

$$\tilde{s} = up^\sigma \tag{13}$$

is a factorization of $\tilde{s}$ as in (7), so that u is an invertible element. For this particular value of $\tilde{s}$, the second coordinate of the vector given in (12) equals

$$\tilde{t}up^{\varepsilon-\delta+\sigma}. \tag{14}$$

There are two cases as $\tilde{t}$ varies in $\{1, 2, \ldots, p^\delta\}$, which are as follows.

$\sigma \leqslant \delta$: here (14) assumes the mutually distinct values

$$up^{\varepsilon-\delta+\sigma}, \qquad 2up^{\varepsilon-\delta+\sigma}, \ldots, (p^{\delta-\sigma} - 1)up^{\varepsilon-\delta+\sigma}, \qquad p^{\delta-\sigma}up^{\varepsilon-\delta+\sigma} = 0 \tag{15}$$

for $\tilde{t} = 1, 2, \ldots, p^{\delta-\sigma}$, and remains 0 for all $\tilde{t} > p^{\delta-\sigma}$.

$\sigma > \delta$: the second summand is zero for all $\tilde{t}$.

We now assume that condition (b) from the theorem is satisfied. So the element p^δ is invertible. This means $\delta = 0$. Consequently, $p^{\varepsilon-\delta} = p^\varepsilon = 0$. Hence, (11) and (12) yield the same set of p^ε vectors.

Finally, assume that (b) is not satisfied. (We did already rule out (a) at the beginning of the proof.) Thus, p^δ is not invertible. This implies $1 \leqslant \delta$. We even have $1 \leqslant \delta < \varepsilon$, since $\delta = \varepsilon$ would give the contradiction $(p^\delta, 0) = (0, 0)$. By (11), the set $(p^\delta, 0)^\perp$ has p^δ vectors

of the form $(p, *)$, whereas (15) shows that the set $U(p^\delta, 0)$ contains only $p^{\delta-1}$ such vectors. Therefore, $U(p^\delta, 0)$ cannot be equal to $(p^\delta, 0)^\perp$. □

As an appendix to the previous proof, we give an explicit example of a vector (b, c) with the property $U(b, c) \neq (b, c)^\perp$. Let $d := 4$, i.e. $p = 2$ and $\varepsilon = 2$. We exhibit the vector $(2, 0) \in \mathbb{Z}_4^2$. In terms of the notation used in theorem 1, we have $\delta = 1 \in \mathbb{Z}$. There are just two points containing $(2, 0)$: these are $\mathbb{Z}_4(1, 0)$ and $\mathbb{Z}_4(1, 2)$. On the other hand, the vector $(2, 2)$ belongs to the perp-set of $(2, 0)$, but it is a multiple neither of $(1, 0)$ nor of $(1, 2)$.

Theorem 4. *Under the assumptions of theorem 3, let (b, c) be a non-zero vector. Then the number of vectors of the set $U(b, c)$ equals*

$$\left(\sum_{\sigma=0}^{\delta-1} (p^{\varepsilon-\sigma} - p^{\varepsilon-\sigma-1}) p^{\delta-\sigma} \right) + p^{\varepsilon-\delta}. \tag{16}$$

Proof. We simplify matters as before by assuming that $(b, c) = (p^\delta, 0)$, where $\delta < \varepsilon$. Choose an integer $\sigma \in \{0, 1, \ldots, \varepsilon\}$. We determine the number of all $\tilde{s} = u p^\sigma \in \mathbb{Z}_d$, where u is any invertible element of $\mathbb{Z}_d$. Observe that in contrast to (13), only σ is now fixed but $\tilde{s}$ is variable. For $\sigma \leqslant \varepsilon - 1$ holds

$$\tilde{s} \in \mathbb{Z}_d \cdot p^\sigma \setminus \mathbb{Z}_d \cdot p^{\sigma+1}.$$

So $\tilde{s}$ can be chosen in $p^{\varepsilon-\sigma} - p^{\varepsilon-\sigma-1}$ different ways. For $\sigma = \varepsilon$ there is a unique choice for $\tilde{s}$, namely $\tilde{s} = 0$.

Now we select one such $\tilde{s}$. We count how many distinct vectors arise from (12), as $\tilde{t}$ varies from 1 to p^δ. By (15) and the subsequent remark on the case $\sigma > \delta$, this number of vectors equals

$$\begin{aligned} p^{\delta-\sigma} \quad &\text{if} \quad 0 \leqslant \sigma \leqslant \delta - 1, \\ 1 \quad &\text{if} \quad \delta \leqslant \sigma \leqslant \varepsilon. \end{aligned}$$

Note that the result depends only on σ, but not on $\tilde{s}$.

Finally, we regard $\sigma, \tilde{s}, \tilde{t}$ to be variable and count the maximal number of pairs $(\tilde{s}, \tilde{t})$ which give rise to distinct vectors in (12). As σ ranges from 0 to $\delta - 1$, the maximal number of such pairs is given by the sum on the left-hand side of (16). For $\delta < \sigma \leqslant \varepsilon$, we obtain

$$\sum_{\sigma=\delta}^{\varepsilon-1} (p^{\varepsilon-\sigma} - p^{\varepsilon-\sigma-1}) + 1 = p^{\varepsilon-\delta}$$

such pairs. This completes the proof. □

Note that (16) remains meaningful for $(b, c) = (0, 0)$, but it *does not provide the correct number of vectors* for $(0, 0)^\perp = \mathbb{Z}_d^2$. This is due to the fact that in (12) we disregard those points which appear (for $(b, c) = (0, 0)$ only) in the proof of theorem 1, case 2.

4. The case of an arbitrary qudit

Throughout this section, we adopt the assumption that

$$d = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_r^{\varepsilon_r}, \tag{17}$$

where $p_1, p_2, \ldots, p_r$ are $r \geqslant 1$ distinct prime numbers and the exponents $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ are non-negative integers $\geqslant 1$. Furthermore, we let

$$d_k := p_k^{\varepsilon_k} \qquad \text{for all} \quad k \in \{1, 2, \ldots, r\}.$$

It is well known that the ring $(\mathbb{Z}_d, +, \cdot)$ is isomorphic to the outer direct product

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}. \tag{18}$$

An isomorphism is given by assigning to each $x \in \mathbb{Z}_d$ the r-tuple

$$(x^{(1)}, x^{(2)}, \ldots, x^{(r)}) \in \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r},$$

where $x^{(k)} \equiv x \pmod{d_k}$ for all $k \in \{1, 2, \ldots, r\}$. We use this isomorphism to identify $\mathbb{Z}_d$ with the outer direct product given in (18), i.e. we do not distinguish between $x \in \mathbb{Z}_d$ and the r-tuple of its *components* $x^{(k)}$. Addition and multiplication of these r-tuples are carried out componentwise, and calculations in the kth component are understood modulo d_k. Note that we used a representation of $\mathbb{Z}_d$ as the *inner direct product* of r ideals in [1]. In the present paper, we shall not follow that approach.

This representation of $\mathbb{Z}_d$ as a direct product has several straightforward consequences for the $\mathbb{Z}_d$-module $\mathbb{Z}_d^2$: Given a vector $(b, c) \in \mathbb{Z}_d^2$, we define its *component vectors* as $(b^{(k)}, c^{(k)}) \in \mathbb{Z}_{d_k}^2$ for all $k \in \{1, 2, \ldots, r\}$. The *degree* of $(b, c) \in \mathbb{Z}_d^2$ is that r-tuple

$$\delta := (\delta_1, \delta_2, \ldots, \delta_r) \tag{19}$$

which is formed by the degrees of its component vectors (in natural order). Thus, for example, the zero vector of $\mathbb{Z}_d$ is the only vector with degree $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r)$. A vector $(b, c) \in \mathbb{Z}_d$ is admissible if and only if there exist elements $u, v \in \mathbb{Z}_d$ with

$$u^{(k)} b^{(k)} + v^{(k)} c^{(k)} = 1 \qquad \text{for all} \quad k \in \{1, 2, \ldots, r\}.$$

This is equivalent to saying that all component vectors of (b, c) are admissible which in turn means that the degree of (b, c) equals $(0, 0, \ldots, 0)$.

Likewise, each submodule of $\mathbb{Z}_d^2$ can be split into its components. The following important observation is immediate from the above: a submodule of $\mathbb{Z}_d^2$ is free and cyclic (i.e. a point) if and only if all its components are free and cyclic. Thus, the projective line over $\mathbb{Z}_d$ can be viewed as the Cartesian product

$$\mathbb{P}_1(\mathbb{Z}_{d_1}) \times \mathbb{P}_1(\mathbb{Z}_{d_2}) \times \cdots \times \mathbb{P}_1(\mathbb{Z}_{d_r}). \tag{20}$$

This allows us to carry over the results from section 3 to our more general setting.

Of course, each matrix $A \in GL_2(\mathbb{Z}_d)$ can also be split into its *component matrices* $A^{(k)} \in GL_2(\mathbb{Z}_{d_k})$. Lemma 1 implies that the degree of vectors of $\mathbb{Z}_d^2$ is a $GL_2(\mathbb{Z}_d)$-invariant notion. Furthermore, each vector with degree $\delta = (\delta_1, \delta_2, \ldots, \delta_r)$ can be mapped to a vector $(q, 0) \in \mathbb{Z}_d^2$ with $q^{(k)} = p_k^{\delta_k}$ for all $k \in \{1, 2, \ldots, r\}$. Likewise, lemma 2 holds, *mutatis mutandis*, for an arbitrary d.

We are now in a position to extend our theorems 1 and 2.

Theorem 5. *Let the integer d be given as in (17). Also, let (b, c) be a vector of $\mathbb{Z}_d^2$ with degree $\delta = (\delta_1, \delta_2, \ldots, \delta_r)$. We denote by K the set of those indices $k \in \{1, 2, \ldots, r\}$ such that $(b^{(k)}, c^{(k)}) = (0, 0)$. Then the following assertions hold[4].*

(a) The number of points of the projective line $\mathbb{P}_1(\mathbb{Z}_d)$ which contain the vector (b, c) equals

$$\prod_{j \notin K} p_j^{\delta_j} \cdot \prod_{k \in K} \left(p_k^{\varepsilon_k} + p_k^{\varepsilon_k - 1} \right).$$

(b) The perp-set $(b, c)^\perp$ has cardinality

$$|(b, c)^\perp| = \prod_{k=1}^r p^{\varepsilon_k + \delta_k} = d \cdot \prod_{k=1}^r p^{\delta_k}.$$

---

[4] Below we use the shorthand $j \notin K$ for $j \in \{1, 2, \ldots, r\} \backslash K$.

Proof. It suffices to apply theorems 1 and 2 to the component vectors of (b, c) and to multiply the cardinalities which can be read off from there. □

Since each pair (b, c) corresponds to all operators of the form $\omega^a X^b Z^c$, and there are d such operators, as an important corollary we have

Corollary 1. *The number of operators in the generalized Pauli group G which commute with the operator $\omega^a X^b Z^c \in G$ is equal to*

$$d \cdot |(b, c)^{\perp}| = d^2 \cdot \prod_{k=1}^{r} p^{\delta_k}, \tag{21}$$

where $(\delta_1, \delta_2, \ldots, \delta_r)$ is the degree of (b, c).

We may define $U(b, c)$ just in the same way as in section 3 as the set-theoretic union of all points of the projective line $\mathbb{P}_1(\mathbb{Z}_d)$ which contain the vector (b, c). By our identification of $\mathbb{P}_1(\mathbb{Z}_d)$ with the Cartesian product (20), it is immediately clear that theorem 3 also holds, *mutatis mutandis*, for our arbitrary d.

Our last result in this section is the following straightforward generalization of theorem 4.

Theorem 6. *Under the assumptions of theorem 5, let (b, c) be a non-zero vector. Then the number of vectors of the set $U(b, c)$ equals*

$$\prod_{j \notin K} \left(\left(\sum_{\sigma_j=0}^{\delta_j-1} \left(p_j^{\varepsilon_j-\sigma_j} - p_j^{\varepsilon_j-\sigma_j-1} \right) p_j^{\delta_j-\sigma_j} \right) + p_j^{\varepsilon_j-\delta_j} \right) \cdot \prod_{k \in K} d_k^2.$$

Proof. For all $j \notin K$, we can apply theorem 5 in order to obtain the number of vectors in the jth component of $U(b, c)$. For the remaining indices $k \in K$ the kth component of $U(b, c)$ coincides with $\mathbb{Z}_{d_k}^2$, and this is a set with cardinality d_k^2. The proof is now accomplished by multiplying these numbers. □

5. Discussion and conclusion

A detailed study of a single qudit living in the Hilbert space of an arbitrary finite dimension d has been performed in terms of the commutation algebra of the elements of the corresponding generalized Pauli group G. The principal outcome of this analysis is the universal formula for the number of operators commuting with a given one (equation (21)) and its interpretation in terms of the fine structure of the projective line defined over the modular ring $\mathbb{Z}_d$. As each operator of the group G/G' has the unique counterpart in a vector of $\mathbb{Z}_d^2$, it belongs to a certain 'layer' characterized by the degree δ of the corresponding vector (see equation (19)). In light of equation (2), the whole set of the generalized Pauli operators is thus naturally structured into disjoint layers. The uppermost layer, $\delta = (0, 0, \ldots, 0)$, comprises all those operators which correspond to admissible vectors, while all the remaining layers feature operators represented by non-admissible vectors; the lowermost layer, $\delta = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r)$, consisting of d operators of $Z(G)$ (equation (5))[5]. Given the fact that the value of δ is intimately connected with the number of free cyclic submodules of $\mathbb{P}_1(\mathbb{Z}_d)$ shared by a given vector, this layered structure of

---

[5] Very roughly speaking, the greater the value of $\Delta \equiv \delta_1 + \delta_2 + \cdots + \delta_r$, the 'lower' the layer; this and some other novel, and rather unexpected, properties of the structure of finite projective ring lines deserve a careful treatment of their own and will, therefore, be the subject of a separate paper.
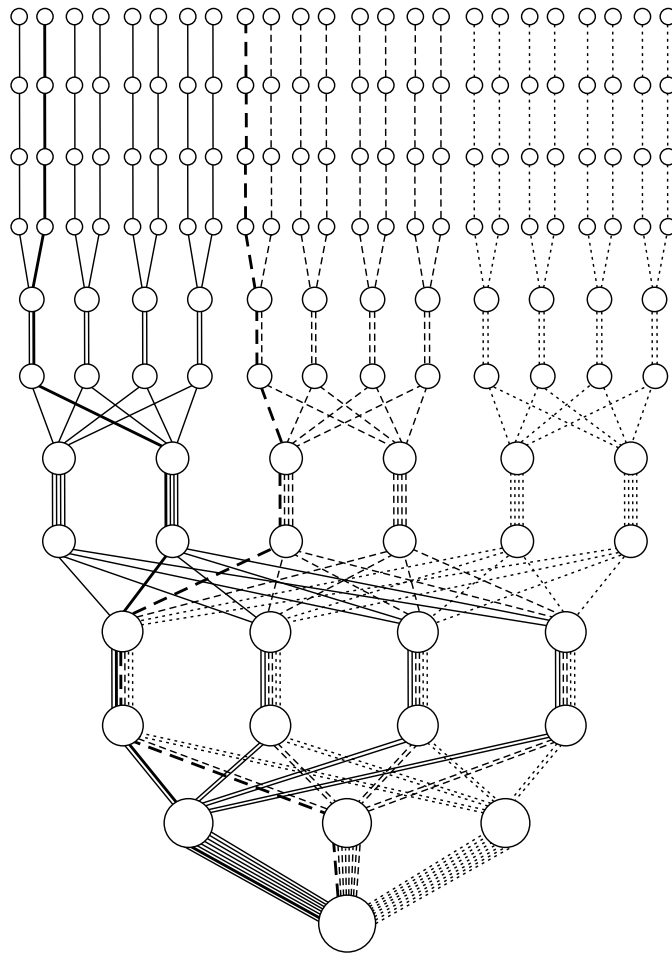
Figure 1. A schematic illustration of the layered structure of the set of the generalized Pauli operators of a 12-dimensional single qudit. Each circle represents d operators $\omega^a X^b Z^c$ with b and c fixed, that is, one vector of $\mathbb{Z}_{12}^2$, and its size increases with the increasing number of free cyclic submodules 'passing' through it. The circles are arranged into 12 horizontal rows; the four rows at the top characterize admissible vectors, the one at the very bottom accommodating all the operators of $Z(G)$. Each free cyclic submodule consists of twelve circles, one from each row, joined by line segments in an obvious way; a couple of them are set in bold so that one can readily recognize a generic shape. A layer is created by the circles of the same size. It can easily be discerned that this particular qudit features six layers characterized (top to bottom) by the following values of $\delta = (\delta_1, \delta_2)$: (0,0), (0,1), (1,0), (0,2), (1,1) and (1,2) and having the following cardinalities (in multiples of 12): 96, 24, 12, 8, 3 and 1, respectively. (Three different kinds of shading of line segments are used only to make the case more illustrative.)

the operators' set can be given a nice geometrical representation, as illustrated in figure 1 for $d = 12$ (i.e. for $p_1 = 3$, $p_2 = 2$, $\varepsilon_1 = 1$ and $\varepsilon_2 = 2$). This representation acquires an especially remarkable form when d is a product of distinct primes [1], i.e. when $\varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_r = 1$ ($r > 1$). In this case r-tuples $(\delta_1, \delta_2, \ldots, \delta_r)$ of *non*-admissible vectors can be regarded as coordinates of the points of the $(r - 1)$-dimensional projective space over $\mathbb{Z}_2$, $PG(r - 1, 2)$, which means that each 'non-admissible' *layer* of the generalized Pauli operators corresponds

to a *point* of $PG(r-1, 2)$; note that this correspondence is sensitive only to the number of factors in (17), not to the values of the factors themselves.

From a physical point of view, it is interesting to mention the maximal sets of mutually perpendicular vectors, also known as the maximal sets of mutually commuting Pauli operators. Obviously, any free cyclic submodule $\mathbb{Z}_d(b, c)$ with (b, c) admissible is such a set. Yet, there are also others; for example, over $\mathbb{Z}_4$ we find the set $\{(0, 0), (2, 2), (2, 0), (0, 2)\}$ that is not a free cyclic submodule. So the question of the properties and cardinalities of such sets for a generic case is a challenging open problem.

Next, an interesting technical aspect of our approach should be emphasized. The attentive reader might have noted that although we started with vectors of $\mathbb{Z}_d^2$ and their symplectic module, we finally (theorem 3) reformulated the problem of finding the perp-set $(b, c)^{\perp}$ in purely geometrical terms, by just employing the points of the projective line $\mathbb{P}_1(\mathbb{Z}_d)$ containing (b, c) and their span. This is, however, in marked contrast to how multiple-qudit cases are handled [7, 8] for there symplectic form is essential—even in the simplest, multiple-qubit cases [9]. This means that although for our *single* qudits the [.,.] form seems to be a redundant concept, it is expected to play a crucial role when extending this approach to tensorial-qudit cases.

As a concluding remark, we would like to stress that it is the above-discussed layered structure of generalized Pauli operators which, in our opinion, is a major feature distinguishing a single d-qudit from a 'tensorial' multi-qudit of the same dimension. Here, the $d = 4$ case can serve as an elementary illustration of this fact; while our single 4-qudit is characterized by two non-trivial layers (disregarding the trivial $Z(G)$-layer) which are embodied in the structure of the projective line over $\mathbb{Z}_4$, a 2-qubit features just a single layer since the geometry behind the corresponding tensor products of the classical Pauli matrices is that of the generalized quadrangle of order 2 [10–12]. Rephrased in more algebraic terms, in the single 4-qudit case the Pauli group contains an element of order 4 (the 'shift' operator), which permutes the four basis vectors cyclically. But it is easy to check that there is no such operator in the two-qubit Pauli group; that is, we work in the regime of characteristic 4 in the former case and that of characteristic 2 in the latter one. Similar comparisons can also be made for several other low-dimensional quantum systems [9, 13, 14]. These should prove helpful when extending this group-geometrical approach to the most general case of multiple qudits.

Acknowledgments

References

[1] Havlicek H and Saniga M 2007 Projective ring line of a specific qudit *J. Phys. A: Math. Theor.* **40** F943–52 (*Preprint* 0708.4333)
[2] Blunck A and Havlicek H 2000 Projective representations: I. Projective lines over rings *Abh. Math. Sem. Univ. Hamburg* **70** 287–99
[3] Havlicek H 2006 Divisible designs, Laguerre geometry, and beyond *Quaderni del Seminario Matematico di Brescia* **11** 1–63 available from http://www.geometrie.tuwien.ac.at/havlicek/pdf/dd-laguerre.pdf
[4] Saniga M, Planat M, Kibler M R and Pracna P 2007 A classification of the projective lines over small rings *Chaos Solitons Fractals* **33** 1095–102

[5] Herzer A 1995 Chain geometries *Handbook of Incidence Geometry* ed F Buekenhout (Amsterdam: Elsevier) pp 781–842

[6] Blunck A and Herzer A 2005 *Kettengeometrien—Eine Einführung* (Aachen: Shaker-Verlag)

[7] Thas K 2007 Pauli operators of *N*-qubit Hilbert spaces and the Saniga–Planat conjecture, Chaos, Solitons and Fractals, submitted

[8] Thas K 2007 The geometry of generalized Pauli operators of *N*-qudit Hilbert space, unpublished

[9] Saniga M and Planat M 2007 Multiple qubits as symplectic polar spaces of order two *Adv. Stud. Theor. Phys.* **1** 1–4

[10] Saniga M, Planat M and Pracna P 2007 Projective ring line encompassing two-qubits *Theor. Math. Phys.* (*Preprint* quant-ph/0611063) at press

[11] Planat M and Saniga M 2007 Pauli graph and finite projective lines/geometries *Proc. SPIE* **6583** 65830W

[12] Planat M and Saniga M 2008 On the Pauli graphs of *N*-qudits *Quantum Inf. Comput.* **8** 127–46

[13] Planat M, Baboin A-C and Saniga M 2007 Multi-line geometry of qubit/qutrit and higher order Pauli operators *Int. J. Theor. Phys.* (*Preprint* 0705.2538) at press

[14] Planat M and Baboin A-C 2007 Qudits of composite dimension, mutually unbiased bases and projective ring geometry *J. Phys. A: Math. Theor.* **40** F1005–12 *Preprint* 0709.2623