View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by HAL-IN2P3

The isotropic lines of $\mathbb{Z}_d^2$

Olivier Albouy[1,2,3]

[1] Université de Lyon, F-69622, Lyon, France
[2] Université Lyon 1, Villeurbanne, France
[3] CNRS/IN2P3, UMR5822, Institut de Physique Nucléaire de Lyon, France

E-mail: o.albouy@ipnl.in2p3.fr

Abstract

We show that the isotropic lines in the lattice $\mathbb{Z}_d^2$ are the Lagrangian submodules of that lattice and we give their number together with the number of them through a given point of the lattice. The set of isotropic lines decompose into orbits under the action of $\mathrm{SL}(2, \mathbb{Z}_d)$. We give an explicit description of those orbits as well as their number and their respective cardinalities. We also develop two group actions on the group $\Sigma_{\mathscr{D}}(M)$ related to the topic.

PACS numbers: 03.65.Fd, 02.10.Ox, 02.10.Ud, 03.67.-a
Keywords: discrete Wigner distributions - isotropic lines - Lagrangian submodules

Introduction

Wigner distributions are a major tool of quantum mechanics. They offer a useful, alternative way besides density matrices of representing pure and mixed states of a quantum system. But whereas in the continuous phase space those distributions are well-defined [1][2], there is still a need for a sound mathematical definition over a discrete phase space. In particular, the structure of such a phase space is of some importance. In 1974, Buot introduced a Wigner distribution over an $d \times d$ phase space with d an odd integer [3]. In 1980, Hannay and Berry followed another approach to build a Wigner distribution over a $2d \times 2d$ lattice [4]. Still in another way, in 2004, Gibbons *et al.* constructed Wigner distributions over a finite field parametrised lattice [5].

More recently, in their way to set up discrete Wigner distributions on the discrete phase space $\mathbb{Z}_d^2$, with $\mathbb{Z}_d$ the set of integers modulo d, Chaturvedi *et al* [6] encountered undetermined signs $S(q, p)$, one at each point (q, p) of the lattice. A natural question then arises: To what extent can these signs be fixed by demanding that averages of Wigner distributions over isotropic lines in the lattice yield probabilities, where an isotropic line is a set of d points on the lattice such that the symplectic product of any two of them is 0 (modulo d). In order to answer this and related questions one needs a detailed knowledge of the structure of the isotropic lines in $\mathbb{Z}_d^2$. In particular, it would be useful to know their number as a whole or with special conditions and also how they arrange in orbits under the action of the symplectic group $\mathrm{SL}(2,\mathbb{Z}_d)$.

This communication is only concerned with the mathematical properties of the isotropic lines in $\mathbb{Z}_d^2$. In Section 1, we derive the number of isotropic lines in $\mathbb{Z}_d^2$ and then in Section 2 the number of them through a given point of the lattice. This should be compared with the results obtained by Havlicek and Saniga in [7] and [8] about the number of projective points in the lattice and the number of them under the same condition. In Section 3, we give a full description of the orbits of isotropic lines under the action of $\mathrm{SL}(2,\mathbb{Z}_d)$ with the help of some parameters. All that is achieved on the basis of a work by the author on symplectic reduction of matrices and Lagrangian submodules [9]. In a fourth section, we develop two group actions on the group $\Sigma_{\mathscr{D}}(M)$ relevant to the understanding of that latter group. For any result appearing in this communication without proof, the reader is referred to [9].

To end this introduction, we note two features of the results presented here. On the one hand, they do not depend on the parity of d, contrary to what happened in [3] and [4]. On the other hand, they have direct relevance to the commuting subgroups of the Pauli group for a general d. That latter feature has been of great importance in the building up of both Wigner ditrbutions and mutually unbiased bases [5][10].

1 The number of isotropic lines

Let ω denote the symplectic product of two vectors of $\mathbb{Z}_d^2$. With matrices, it consists in computing a determinant:

$$\omega((\alpha,\beta),(\gamma,\delta)) = \begin{vmatrix} \alpha & \gamma \\ \beta & \delta \end{vmatrix} = \alpha\delta - \beta\gamma. \tag{1}$$

The orthogonal of a submodule M of $\mathbb{Z}_d^2$ will be denoted M^ω:

$$M^\omega = \{x \in \mathbb{Z}_d^2; \forall y \in M, \omega(x,y) = 0\}. \tag{2}$$

Isotropic submodules are defined to satisfy the set inclusion $M \subset M^\omega$. Lagrangian submodules are the maximal isotropic submodules for inclusion, what is equivalent to $M = M^\omega$.

In a first time, we are going to find the number of isotropic lines in $\mathbb{Z}_d^2$ for d a power of a prime, say $d = p^s$, $s \geq 1$. The way we derive this number is a strict application of Theorem 7 in [9]. This brings about a hint for Section 4, but we shall also see that there exists a shortcut. We then address the case of a general d.

1.1 Special case: d a power of a prime

Let $\widetilde{s} = \lfloor s/2 \rfloor$, the floor part of $s/2$. As shown in [9], for any Lagrangian submodule M, there exist $S \in \mathrm{SL}(2, \mathbb{Z}_{p^s})$ and $k \in \{0, \ldots, \widetilde{s}\}$ such that M is linearly generated by the column vectors of

$$S \times \begin{pmatrix} p^k & 0 \\ 0 & p^{s-k} \end{pmatrix}. \tag{3}$$

In other words, with S_1 and S_2 the two column vectors of S, (S_1, S_2) is a symplectic computational basis of $(\mathbb{Z}_{p^s})^2$ and M is the set of all linear combinations of $p^k S_1$ and $p^{s-k} S_2$ with coefficients in $\mathbb{Z}_{p^s}$. As a converse, any submodule thus generated is Lagrangian. In fact, the number k is a property of M, that is to say for any convenient pair (S, k') in order to generate M as in (3), we have $k' = k$. We will denote $\mathbf{O}_k(p^s)$ the set of all Lagrangian submodules thus obtained for a given k and S varying. The cardinality of any $M \in \mathbf{O}_k(p^s)$ is

$$p^{(s-1)-(k-1)} p^{(s-1)-(s-k-1)} = p^s. \tag{4}$$

Let ℓ be an isotropic line and $\langle \ell \rangle$ the submodule it generates, the set of all finite linear combinations of vectors of ℓ. Any two vectors in $\langle \ell \rangle$ are orthogonal and hence $\langle \ell \rangle$ is an isotropic submodule containing at least p^s vectors. Thus isotropic lines and Lagrangian submodules are the same.

The number of free vectors x in $\mathbb{Z}_{p^s}$ is $p^{2s} - p^{2(s-1)}$. The number of vectors y such that for a given free x we have $\omega(x, y) = 1$ is p^s. The number of pairs (x, y) such that $\omega(x, y) = 1$ is the product of the two previous ones:

$$n_\omega = |\mathrm{SL}(2, \mathbb{Z}_{p^s})| = p^{3s} - p^{3s-2}. \tag{5}$$

Several symplectic matrices S may give rise to the same submodule in $\mathbf{O}_k(p^s)$ according to the form (3). Let $k \in \{0, \ldots, \widetilde{s}\}$ and $M \in \mathbf{O}_k(p^s)$. Let $\Sigma_{\mathscr{D}}(M)$ be the matrix group of the changes of computational basis such that if $P \in \Sigma_{\mathscr{D}}(M)$ and if M is generated by the column vectors of the matrix given in (3), then M is also generated by the column vectors of the matrix

$$SP \times \begin{pmatrix} p^k & 0 \\ 0 & p^{s-k} \end{pmatrix}, \tag{6}$$

where SP need not be symplectic. In fact, we derived in [9] that the group $\Sigma_{\mathscr{D}}(M)$ is completely determined by the value of k. So, the number of symplectic matrices that give rise to a given $M \in \mathbf{O}_k(p^s)$ is

$$n_{\mathscr{D}}(k) = |\Sigma_{\mathscr{D}}(M) \cap \mathrm{SL}(2, \mathbb{Z}_{p^s})| \tag{7}$$

and hence

$$|\mathbf{O}_k(p^s)| = \frac{n_\omega}{n_{\mathscr{D}}(k)}. \tag{8}$$

Let us suppose that $2k < s$. In $\Sigma_{\mathscr{D}}(M)$, the number of matrices with determinant 1 is the same as the number of matrices with any other (invertible) determinant. Indeed, if $u \in U(\mathbb{Z}_{p^s})$ and $P = (P_1|P_2) \in \Sigma_{\mathscr{D}}(M) \cap \mathrm{SL}(2, \mathbb{Z}_{p^s})$, with P_1 and P_2 the first and second columns of P respectively, then $(uP_1|P_2) \in \Sigma_{\mathscr{D}}(M)$ but with determinant u. This transformation is injective so that the number of matrices in

$\Sigma_{\mathscr{D}}(M)$ with determinant u is greater than or equal to the number of matrices in $\Sigma_{\mathscr{D}}(M)$ with determinant 1. The converse inequality may be shown the same way. So we have

$$\begin{aligned} n_{\mathscr{D}}(k) &= \frac{|\Sigma_{\mathscr{D}}(M)|}{|U(\mathbb{Z}_{p^s})|} = \frac{(p^s - p^{s-1})^2 \cdot p^{(s-1)-(s-2k-1)} \cdot p^s}{p^s - p^{s-1}} = (p^s - p^{s-1})p^{s+2k} && \text{(9a)} \\ &= p^{2s}(p^{2k} - p^{2k-1}) && \text{(9b)} \end{aligned}$$

and so

$$|\mathbf{O}_k(p^s)| = \frac{p^s - p^{s-2}}{p^{2k} - p^{2k-1}} = p^{s-2k-1}(p+1). \tag{10}$$

If $2k = s$ (what supposes that s is even), then $\Sigma_{\mathscr{D}}(M) \cap \mathrm{SL}(2, \mathbb{Z}_{p^s}) = \mathrm{SL}(2, \mathbb{Z}_{p^s})$ and so

$$\left|\mathbf{O}_{s/2}(p^s)\right| = \frac{n_\omega}{n_\omega} = 1. \tag{11}$$

For s odd, then $2\widetilde{s} = s - 1$,

$$\sum_{k=0}^{\widetilde{s}} p^{-2k} = \frac{1 - p^{-2(\widetilde{s}+1)}}{1 - p^{-2}} = \frac{p^{2(\widetilde{s}+1)} - 1}{p^{2(\widetilde{s}+1)} - p^{2\widetilde{s}}} = \frac{p^{s+1} - 1}{p^{s+1} - p^{s-1}} \tag{12}$$

and hence the number of isotropic lines is

$$n_L(p^s) = \sum_{k=0}^{\widetilde{s}} |\mathbf{O}_k(p^s)| = p^{s-1}(p+1)\frac{p^{s+1} - 1}{p^{s+1} - p^{s-1}} = \frac{p^{s+1} - 1}{p - 1}. \tag{13}$$

If s is even, then $2\widetilde{s} = s$,

$$\sum_{k=0}^{\widetilde{s}-1} p^{-2k} = \frac{1 - p^{-2\widetilde{s}}}{1 - p^{-2}} = \frac{p^{2\widetilde{s}} - 1}{p^{2\widetilde{s}} - p^{2\widetilde{s}-2}} = \frac{p^s - 1}{p^s - p^{s-2}} \tag{14}$$

and hence the number of isotropic lines is again

$$\begin{aligned} n_L(p^s) = \sum_{k=0}^{\widetilde{s}-1} |\mathbf{O}_k(p^s)| + 1 &= p^{s-1}(p+1)\frac{p^s - 1}{p^s - p^{s-2}} + 1 \\ &= p\frac{p^s - 1}{p - 1} + 1 = \frac{p^{s+1} - p + p - 1}{p - 1} = \frac{p^{s+1} - 1}{p - 1}. && \text{(15)} \end{aligned}$$

1.2 General case: d any integer ≥ 2

Now let d be any integer greater than or equal to 2 and

$$d = \prod_{i \in I} p_i^{s_i} \tag{16}$$

be the prime factor decomposition of d. Due to the Chinese remainder theorem, we can study the structure of an isotropic line ℓ in each of the Chinese factor $(\mathbb{Z}_{p_i^{s_i}})^2$. For every $i \in I$, let $\ell_i = \pi_{p_i}(\ell)$ be the i-th Chinese projection of ℓ. As a subgroup of $(\mathbb{Z}_{p_i^{s_i}})^2$, $\langle \ell_i \rangle$ has cardinality a power of p_i, say $p_i^{t_i}$. As an isotropic submodule of $(\mathbb{Z}_{p_i^{s_i}})^2$, $\langle \ell_i \rangle$ is included in a Lagrangian submodule and then $t_i \leq s_i$. So

$$d = |\ell| \leq \prod_{i \in I} |\ell_i| \leq \prod_{i \in I} p_i^{t_i} \leq d, \tag{17}$$

what proves that $t_i = s_i$. Moreover, if $\ell_i \subsetneq \langle \ell_i \rangle$ for some i, the second inequality just above would be strict, what is impossible and so $\ell_i = \langle \ell_i \rangle$ is a Lagrangian submodule of $(\mathbb{Z}_{p_i^{s_i}})^2$. As to the converse, for all $i \in I$, let ℓ'_i be a Lagrangian submodule of $(\mathbb{Z}_{p_i^{s_i}})^2$. The set ℓ' of all vectors $x \in \mathbb{Z}_d^2$ such that for all i, $\pi_{p_i}(x) \in \ell'_i$, is an isotropic set with cardinality d, namely an isotropic line. The reader may check that the maps $\ell \mapsto (\ell_i)_{i \in I}$ and $(\ell'_i)_{i \in I} \mapsto \ell'$ thus defined are reciprocal of one another.

So, isotropic lines and Lagrangian submodules are the same sets of $\mathbb{Z}_d^2$ and the number of isotropic lines of $\mathbb{Z}_d^2$ is

$$n_L(d) = \prod_{i \in I} n_L\left(p_i^{s_i}\right) = \prod_{i \in I} \frac{p_i^{s_i+1} - 1}{p_i - 1}. \tag{18}$$

Remark 1 *In (3), the left-hand-side factor was a symplectic matrix. But in fact, any invertible matrix would be convenient since we are to consider all the linear combinations of the columns in the product. Thus we could have calculated the cardinality of an orbit as*

$$\frac{n_\omega \, |U(\mathbb{Z}_{p^s})|}{|\Sigma_{\mathscr{D}}(M)|} \text{ instead of } \frac{n_\omega}{\left(|\Sigma_{\mathscr{D}}(M)| \,/\, |U(\mathbb{Z}_{p^s})|\right)} \tag{19}$$

and the argument between (8) and (9) could have been avoided.

Remark 2 *Let us assume that s is even. It should be noticed that the formula for the cardinality of $\mathbf{O}_k(p^s)$ given in (10) is not valid for $k = s/2$. Indeed, equation (10) gives $1 + 1/p$ for that particular value of k, what is even not an integer. Equivalently, $n_{\mathscr{D}}(k)$ and $|\Sigma_{\mathscr{D}}(M)|$ have no unique expression for all values of k. This must be traced back to the behaviour of $\Sigma_{\mathscr{D}}(M)$ when k is ranging up to $s/2$ (see [9]).*

2 The number of lines through a given point

We now give the number of isotropic lines through a given point of the lattice. We suppose that $d = p^s$ is a power of a prime. Let $x \in \mathbb{Z}_d^2$ and let $t = v_p(x)$ be the p-valuation of x. Since all the vectors in an isotropic line $\ell \in \mathbf{O}_k(p^s)$ have p-valuation at least k, the vector x cannot be in ℓ unless $k \leq t$. Let us assume that k is such that $s - k \leq t$, what implies that $k \leq t$. Then for any computational basis (f_1, f_2), symplectic or not, x is a linear combination of $p^k f_1$ and $p^{s-k} f_2$. Hence

$$\forall k \in \{0, \dots, \lfloor s/2 \rfloor\}, \forall \ell \in \mathbf{O}_k(p^s), (k \geq s - t \Longrightarrow x \in \ell). \tag{20}$$

That case can occur only if $t \geq \lceil s/2 \rceil$, the ceiling part of $s/2$. Now, let us assume that k is such that $k \leq t < s - k$. Thus $2k < s$ and we search for the symplectic computational bases (f_1, f_2) such that x is a linear combination of $p^k f_1$ and $p^{s-k} f_2$. Let (f_1, f_2) be a symplectic computational basis and $x = af_1 + bf_2$. Since

$$v_p(\omega(x, f_2)) = v_p(a) \geq t \geq k, \tag{21}$$

we have no extra conditions on the choice of f_2. But we must have

$$v_p(\omega(x, f_1)) = v_p(b) \geq s - k, \tag{22}$$

what shows that in a symplectic basis where $x = (p^t, 0)$, f_1 must be of the form

$$f_1 = (\alpha, \beta p^{s-k-t}), \tag{23}$$

with $\alpha, \beta \in \mathbb{Z}_d$. The number of suitable vectors f_1 is

$$(p^s - p^{s-1}) \cdot p^{(s-1)-(s-k-t-1)} = (p^s - p^{s-1})p^{k+t}. \tag{24}$$

The number of suitable vectors f_2 for a given f_1 is p^s. Then the number of suitable, symplectic computational bases (f_1, f_2) is $(p^s - p^{s-1})p^{s+k+t}$. Moreover, if f is a convenient basis and

$$\left\langle p^k f_1, p^{s-k} f_2 \right\rangle = \left\langle p^k f_1', p^{s-k} f_2' \right\rangle, \tag{25}$$

then f' is convenient too. With (9a), we deduce that the number of isotropic lines in $\mathbf{O}_k(p^s)$ containing x is

$$\frac{(p^s - p^{s-1})p^{s+k+t}}{(p^s - p^{s-1})p^{s+2k}} = p^{t-k}. \tag{26}$$

Thus, if $t < \lceil s/2 \rceil$, the number of isotropic lines containing x is

$$\sum_{k=0}^{t} p^{t-k} = p^t \cdot \frac{1 - p^{-(t+1)}}{1 - p^{-1}} = \frac{p^{t+1} - 1}{p - 1}. \tag{27}$$

If $t \geq \lceil s/2 \rceil$ and $\widetilde{s} = \lfloor s/2 \rfloor$, the number of isotropic lines containing x is

$$\sum_{k=0}^{s-t-1} p^{t-k} + \sum_{k=s-t}^{\widetilde{s}} \left| \mathbf{O}_k(p^s) \right|. \tag{28}$$

The first term is equal to

$$p^t \cdot \frac{1 - p^{-(s-t)}}{1 - p^{-1}} = \frac{p^{t+1} - p^{2t-s+1}}{p - 1}. \tag{29}$$

For s odd, then $2\widetilde{s} = s - 1$,

$$\sum_{k=s-t}^{\widetilde{s}} p^{-2k} = p^{-2(s-t)} \cdot \frac{1 - p^{-2(\widetilde{s}-s+t+1)}}{1 - p^{-2}} = \frac{p^{2t-s+1} - 1}{p^{s-1}(p^2 - 1)}, \tag{30}$$

and the second term in (28) is equal to

$$p^{s-1}(p+1)\frac{p^{2t-s-1} - 1}{p^{s-1}(p^2 - 1)} = \frac{p^{2t-s+1} - 1}{p - 1}. \tag{31}$$

For s even, then $2\widetilde{s} = s$,

$$\sum_{k=s-t}^{\widetilde{s}-1} p^{-2k} = p^{-2(s-t)} \cdot \frac{1 - p^{-2(\widetilde{s}-1-s+t+1)}}{1 - p^{-2}} = \frac{p^{2t-s+1} - p}{p^{s-1}(p^2 - 1)}, \tag{32}$$

and the second term in (28) is again

$$p^{s-1}(p+1)\frac{p^{2t-s+1} - p}{p^{s-1}(p^2 - 1)} + 1 = \frac{p^{2t-s+1} - 1}{p - 1}. \tag{33}$$

Hence, in any case, the number of isotropic lines containing some given vector x with p-valuation t is

$$n_L(p^s; x) = n_L(p^s; t) = \frac{p^{t+1} - 1}{p - 1}. \tag{34}$$

In particular,

$$n_L(p^s; t = 0) = 1 \text{ and } n_L(p^s; t = s) = n_L(p^s). \tag{35}$$

That is to say the sole isotropic line containing a free vector is the submodule it generates and every isotropic line goes through the null vector.

If d is not necessarily a power of a prime, then with (16) and for all i, $t_i = v_{p_i}(x)$, we obtain that the number of isotropic lines containing x is

$$n_L(d; x) = n_L(d; (t_i)_{i\in I}) = \prod_{i\in I} \frac{p_i^{t_i+1} - 1}{p_i - 1}. \tag{36}$$

3 Orbits under the action of $\mathrm{SL}(2, \mathbb{Z}_d)$

As in Section 1, we first suppose that d is a power of a prime, say $d = p^s$, $s \geq 1$. Then it is obvious from (3) that the orbits of the left-action of $\mathrm{SL}(2, \mathbb{Z}_{p^s})$ among the isotropic lines are the $\mathbf{O}_k(p^s)$. Their number is $\lfloor s/2 \rfloor + 1$ and we have already seen what their cardinalities are in (10) and (11).

Now if d is a composite integer as in (16), then the set of the orbits is parametrised by

$$k = (k_i)_{i\in I} \in \prod_{i\in I}\{0, \dots, \lfloor s_i/2 \rfloor\} \tag{37}$$

and the orbit with index k is

$$\mathbf{O}_k(d) = \left\{\ell \subset \mathbb{Z}_d^2; |\ell| = N, \pi_{p_i}(\ell) \in \mathbf{O}_{k_i}(p_i^{s_i})\right\}. \tag{38}$$

The number of orbits is

$$\prod_{i\in I} (\lfloor s_i/2 \rfloor + 1), \tag{39}$$

and the cardinality of one of them is

$$|\mathbf{O}_k(d)| = \prod_{i\in I} |\mathbf{O}_{k_i}(p_i^{s_i})|. \tag{40}$$

Example *Let us suppose that d contains no square factor, that is to say in (16), for all $i \in I$, $s_i = 1$. According to (3), with k necessarily equal to 0, the isotropic lines are the submodules that can be generated by a single free vector. These submodules are called the projective points of $\mathbb{Z}_d^2$. With (18), we find that the number of isotropic lines is*

$$n_L(d) = \prod_{i \in I}(p_i + 1). \tag{41}$$

They all belong to the sole orbit under the action of $\mathrm{SL}(2, \mathbb{Z}_d)$ corresponding to $k_i = 0$ for all i.

4 Some group actions on $\Sigma_{\mathscr{D}}(M)$

In this section, we assume that $d = p^s$ is a power of a prime. In order to establish equation (9), we showed that the number of matrices in $\Sigma_{\mathscr{D}}(M)$ with determinant 1 is the same as the number of matrices in the same set with any other (invertible) determinant. The simple reasoning we used was enough in the frame of Section 1. But we are going to introduce here two other group actions that are linked to that point and to Remarks 1 and 2. Let ρ_0 be the action of $U(\mathbb{Z}_{p^s})$ on $\Sigma_{\mathscr{D}}(M)$ defined by

$$\forall u \in U(\mathbb{Z}_{p^s}), \forall P = (P_1|P_2) \in \Sigma_{\mathscr{D}}(M), \rho_0(u) \cdot P = (uP_1|u^{-1}P_2) \tag{42}$$

and ρ_1 the action of $U(\mathbb{Z}_{p^s})^2$ on $\Sigma_{\mathscr{D}}(M)$ defined by

$$\forall (u_1, u_2) \in U(\mathbb{Z}_{p^s})^2, \forall P = (P_1|P_2) \in \Sigma_{\mathscr{D}}(M), \rho_1(u_1, u_2) \cdot P = (u_1P_1|u_2P_2). \tag{43}$$

All the orbits of ρ_0 (resp. ρ_1) have the same cardinality, namely $|U(\mathbb{Z}_{p^s})| = p^s - p^{s-1}$ (resp. $|U(\mathbb{Z}_{p^s})|^2$). In a given orbit of ρ_0, every matrix has the same determinant. Since $\mathbb{Z}_{p^s}$ is a commutative ring, those two actions "commute":

$$\rho_1(u_1, u_2) \cdot (\rho_0(u) \cdot P) = \rho_0(u) \cdot (\rho_1(u_1, u_2) \cdot P). \tag{44}$$

Let $(u_1, u_2), (v_1, v_2) \in U(\mathbb{Z}_{p^s})^2$ such that $u_1u_2 = v_1v_2$, that is to say

$$\forall P \in \Sigma_{\mathscr{D}}(M), \det(\rho_1(u_1, u_2) \cdot P) = \det(\rho_1(v_1, v_2) \cdot P). \tag{45}$$

With $\lambda = u_2v_2^{-1} = u_1^{-1}v_1 \in U(\mathbb{Z}_{p^s})$, we have

$$(v_1, v_2) = (\lambda u_1, \lambda^{-1}u_2). \tag{46}$$

Thus we have a kind of a discrete Hopf fibration. It is given by the action h of $U(\mathbb{Z}_{p^s})$ on $U(\mathbb{Z}_{p^s})^2$ defined by

$$\forall \lambda \in U(\mathbb{Z}_{p^s}), \forall (u_1, u_2) \in U(\mathbb{Z}_{p^s})^2, h(\lambda) \cdot (u_1, u_2) = (\lambda u_1, \lambda^{-1}u_2). \tag{47}$$

Moreover, the action $\rho = \rho_1/(h, \rho_0)$ of $U(\mathbb{Z}_{p^s})^2/h$ on $\Sigma_{\mathscr{D}}(M)/\rho_0$ is well-defined. For any $u \in U(\mathbb{Z}_{p^s})$, let

$$D_u = \{P \in \Sigma_{\mathscr{D}}(M); \det P = u\}. \tag{48}$$

Every orbit of ρ is transversal to D_u/ρ_0. Indeed, let P be in some orbit O of ρ_1 with some determinant v. Then $(uv^{-1}P_1|P_2)$ is in O with determinant u so that there is at least one orbit of ρ_0 in $D_u \cap O$. Then if P and $Q = (u_1P_1|u_2P_2)$ are in O and have the same determinant, then $u_2 = u_1^{-1}$ and thus P and Q are in the same orbit of ρ_0.

As a conclusion, we have a partition $E = \{E_{ij}\}$ of $\Sigma_{\mathscr{D}}(M)$: The E_{ij}'s are the orbits of ρ_0, $i \in U(\mathbb{Z}_{p^s})$ is the determinant of every matrix in E_{ij} and j stands for an orbit of ρ_1 (or equivalently of ρ). The number of different values that j can assume is

$$n_\rho = \frac{|\Sigma_{\mathscr{D}}(M)|}{|U(\mathbb{Z}_{p^s})|^2}. \tag{49}$$

If $2k < s$, then $n_\rho = p^{s+2k}$ according to (9a). But if $k = s/2$, then

$$n_\rho = \frac{|\mathrm{GL}(2, \mathbb{Z}_{p^s})|}{|U(\mathbb{Z}_{p^s})|^2} = \frac{(p^{2s} - p^{2(s-1)}) \cdot (p^s - p^{s-1}) \cdot p^s}{(p^s - p^{s-1})^2} = p^{2s} + p^{2s-1} > p^{2s}. \tag{50}$$

Let $P \in E_{i_1j_1}$ and $Q \in E_{i_2j_2}$. On the one hand, $\det P = i_1$ and $\det Q = i_2$. On the other hand, $j_1 = j_2$ iff Q_1 and Q_2 are proportional to P_1 and P_2 respectively. In passing, we find again that the number of matrices in $\Sigma_{\mathscr{D}}(M)$ with some determinant u is the same as the number of matrices in $\Sigma_{\mathscr{D}}(M)$ with any other (invertible) determinant v.

Acknowledgments

The author wishes to thank Subhash Chaturvedi for calling his attention to all the features about isotropic lines addressed in this communication and to their involvement in the setting-up of discrete Wigner distributions.

This work is part of the Ph.D. thesis by the author. He is indebted to his advisor for useful comments and also to Michel Planat and Metod Saniga for introducing him to finite geometry in the frame of quantum physics.

References

[1] E. P. Wigner. On the Quantum Correction For Thermodynamic Equilibrium. *Physical Review*, 40:749–759, 1932.

[2] S. de Groot. *La transformation de Weyl et la fonction de Wigner: une forme alternative de la mcanique quantique*. Les Presses Universitaires de Montral, 1975.

[3] F. A. Buot. Method for calculating TrH^n in solid-state theory. *Physical Review B*, 10:3700–3705, 1974.

[4] J. H. Hannay and M. V. Berry. On the Quantum Correction For Thermodynamic Equilibrium. *Physica D*, 1:267, 1980.

[5] K. S. Gibbons, F. J. Hoffman, and W. K. Wootters. Discrete phase space based on finite fields. *Physical Review A*, 70:062101, 2004.

[6] S. Chaturvedi, E. Ercolessi, G. Marmo, G. Morandi, N. Mukunda, and R. Simon. Wigner-Weyl correspondence in quantum mechanics for continuous and discrete systems - a Dirac-inspired view. *Journal of Physics A*, 39:1405–1423, 2006.

[7] H. Havlicek and M. Saniga. Projective Ring Line of a Specific Qudit. *Journal of Physics A*, 40:F943–F952, 2007.

[8] H. Havlicek and M. Saniga. Projective Ring Line of an Arbitrary Single Qudit. *Journal of Physics A*, 41:015302, 2008.

[9] Olivier Albouy. Matrix reduction and Lagrangian submodules. *arXiv:0809.1059v1 [quant-ph].*

[10] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34:512–528, 2002.