

## Symplectic transformations and quantum tomography in finite quantum systems

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

2010 J. Phys. A: Math. Theor. 43 042001

(<http://iopscience.iop.org/1751-8121/43/4/042001>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 171.66.16.157

The article was downloaded on 03/06/2010 at 08:51

Please note that [terms and conditions apply](#).

## FAST TRACK COMMUNICATION

# Symplectic transformations and quantum tomography in finite quantum systems

A Vourdas<sup>1</sup> and C Banderier<sup>2</sup><sup>1</sup> Department of Computing, University of Bradford, Bradford BD7 1DP, UK<sup>2</sup> Laboratoire d'informatique de Paris-Nord, UMR CNRS 7030, Université Paris XIII, Villetaneuse, FranceE-mail: [A.Vourdas@Bradford.ac.uk](mailto:A.Vourdas@Bradford.ac.uk)

Received 18 November 2009, in final form 7 December 2009

Published 4 January 2010

Online at [stacks.iop.org/JPhysA/43/042001](http://stacks.iop.org/JPhysA/43/042001)**Abstract**

Quantum systems where the position and momentum are in the ring  $\mathbb{Z}_d$  ( $d$  is an odd integer) are considered. Symplectic transformations are studied, and the order of  $Sp(2, \mathbb{Z}_d)$  is calculated. Quantum tomography is also discussed. It is shown that measurements (used in the inverse Radon transform) need to be made on  $J_2(d)$  lines (where  $J_2(d)$  is the Jordan totient function).

PACS number: 03.65.Ca

**1. Introduction**

Finite quantum systems where the position and momentum take values in the ring  $\mathbb{Z}_d$  (the integers modulo  $d$ ) have been studied extensively in the literature (reviews with an extensive list of references have been presented in [1–3]). Related mathematical work is presented in [4–7].

When  $d$  is a prime number so that  $\mathbb{Z}_d$  is a field, these systems have stronger properties, in comparison to the case where  $d$  is a non-prime number and  $\mathbb{Z}_d$  is a ring but not a field. All phase space methods known from the harmonic oscillator (symplectic transformations, Wigner and Weyl functions, quantum tomography, etc) can also be applied in the context of finite quantum systems. Most of these techniques rely on the existence of inverses of the parameters. In a ring only  $\varphi(d)$  (the Euler totient function) of the elements have inverses. For this reason the results are stronger in the case where  $\mathbb{Z}_d$  is a field, in comparison to the case where  $\mathbb{Z}_d$  is a ring but not a field.

Related is also the result that the number of mutually unbiased bases [8–15]  $\mathfrak{M}(d)$ , which is known to obey the inequality  $\mathfrak{M}(d) \leq d + 1$ , takes in the case of a field the maximum value  $\mathfrak{M}(d) = d + 1$ .

In this communication, we first consider the symplectic group  $Sp(2, \mathbb{Z}_d)$  [16–19] and calculate its order. We next consider briefly Wigner and Weyl functions [1, 20–24] with

emphasis on their marginal properties. It is well known that there are differences in the formalism for odd and even  $d$ , and everywhere in this communication we consider the case of odd  $d$ . We use these functions in the context of quantum tomography. We show that measurements on  $J_2(d)$  lines give the Weyl function in the full phase space.

In section 2 we discuss the symplectic group and prove proposition 2.1 about its order. In section 3 we discuss briefly quantum systems with positions and momenta in  $\mathbb{Z}_d$ . In section 4 we discuss quantum tomography and prove proposition 4.1. We conclude in section 5 with a discussion of our results.

1.1. The  $\mathbb{Z}_d^*$  group of reduced residue classes modulo  $d$

We consider the ring  $\mathbb{Z}_d$ . An element  $\alpha \in \mathbb{Z}_d$  is invertible if and only if  $\mathfrak{G}(\alpha, d) = 1$  (where  $\mathfrak{G}$  denotes the greatest common divisor). The invertible elements of  $\mathbb{Z}_d$  (called units) form a group with respect to multiplication, which is called the group of reduced residue classes modulo  $d$ , and which we denote as  $\mathbb{Z}_d^*$ . The order of this group is  $|\mathbb{Z}_d^*| = \varphi(d)$ .

Let  $d$  be an integer, which is factorized in terms of  $N$  prime numbers  $p_i$  as

$$d = \prod_{i=1}^N p_i^{e_i}. \tag{1}$$

The Euler totient function is given by

$$\varphi(d) = d \prod_{i=1}^N \left(1 - \frac{1}{p_i}\right). \tag{2}$$

In the case that  $d$  is a prime number  $p$ ,  $\varphi(p) = p - 1$  and  $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ . When  $d$  is a power of a prime number  $p^e$ ,  $\varphi(p^e) = p^e - p^{e-1}$  and the non-invertible elements are  $Np$  where  $N = 0, 1, \dots, p^{e-1} - 1$ . For odd primes,  $\mathbb{Z}_{p^e}^*$  is a cyclic group.

A generalization of the Euler totient function is the Jordan totient function

$$J_k(d) = d^k \prod_{i=1}^N \left(1 - \frac{1}{p_i^k}\right). \tag{3}$$

Clearly  $J_1(d) = \varphi(d)$ . For prime numbers,  $J_k(p) = p^k - 1$ . Below we will use the Jordan totient function

$$J_2(d) = d^2 \prod_{i=1}^N \left(1 - \frac{1}{p_i^2}\right) = \varphi(d)\psi(d), \tag{4}$$

where

$$\psi(d) = d \prod_{i=1}^N \left(1 + \frac{1}{p_i}\right) \tag{5}$$

is the Dedekind  $\psi$ -function.

All  $\varphi(d)$ ,  $J_k(d)$ ,  $\psi(d)$  are multiplicative functions (i.e.  $f(d_1 d_2) = f(d_1) f(d_2)$  for coprime  $d_1, d_2$ ).

2. The  $Sp(2, \mathbb{Z}_d)$  group

In this section we study the  $Sp(2, \mathbb{Z}_d)$  for later use in the context of finite quantum systems. We consider matrices of the type

$$g(\kappa, \lambda | \mu, \nu) \equiv \begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix}; \quad \det(g) = \kappa \nu - \lambda \mu = 1 \pmod{d}; \quad \kappa, \lambda, \mu, \nu \in \mathbb{Z}_d. \tag{6}$$

We can easily verify that the product of two such matrices is a matrix of the same type. Also the inverse matrix exists and is the  $g(v, -\lambda | -\mu, \kappa)$ . Therefore, these matrices form a group which is the  $Sp(2, \mathbb{Z}_d)$  group.

**Proposition 2.1.** *Let  $d$  be an integer, which is factorized in terms of prime numbers, as in equation (1). Then*

$$|Sp(2, \mathbb{Z}_d)| = dJ_2(d). \tag{7}$$

**Proof.** We first take  $d = p^e$  and we prove that

$$|Sp(2, \mathbb{Z}_d)| = d^2\varphi(d) \left(1 + \frac{1}{p}\right). \tag{8}$$

In order to prove this, we give below two non-overlapping subsets of  $Sp(2, \mathbb{Z}_d)$  (where  $\kappa \in \mathbb{Z}_d^*$ , and  $\kappa = Np$ ) and their cardinalities:

$$\begin{aligned} S_1 &= \{g(\kappa, \lambda | \mu, \kappa^{-1}(1 + \lambda\mu)) \mid \kappa \in \mathbb{Z}_{p^e}^*; \lambda, \mu \in \mathbb{Z}_d\}; & |S_1| &= d^2\varphi(d) \\ S_2 &= \left\{g(Np, \lambda | \mu, \nu) \mid N = 0, 1, \dots, \frac{d}{p} - 1; \lambda, \mu \in \mathbb{Z}_d^*; \nu \in \mathbb{Z}_d\right\}; & |S_2| &= d^2\varphi(d) \frac{1}{p}. \end{aligned} \tag{9}$$

In  $S_2$  we have  $\lambda\mu = Np\nu - 1$  and this shows that  $\lambda, \mu$  are invertible elements and therefore  $|S_2| = d^2\varphi(d) \frac{1}{p}$ . Adding these two cardinalities we prove equation (8).

We next show that  $v(d) \equiv |Sp(2, \mathbb{Z}_d)|$  is a multiplicative function. The proof is based on the following bijection between  $Sp(2, \mathbb{Z}_d)$  with  $d = d_1d_2$  where  $d_1, d_2$  are coprime, and  $Sp(2, \mathbb{Z}_{d_1}) \times Sp(2, \mathbb{Z}_{d_2})$ :

$$\begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix} \mapsto \left( \begin{pmatrix} \kappa_1 & \lambda_1 \\ \mu_1 & \nu_1 \end{pmatrix}, \begin{pmatrix} \kappa_2 & \lambda_2 \\ \mu_2 & \nu_2 \end{pmatrix} \right) \tag{10}$$

where

$$\kappa_i = \kappa \pmod{d_i}; \quad \lambda_i = \lambda \pmod{d_i}; \quad \mu_i = \mu \pmod{d_i}; \quad \nu_i = \nu \pmod{d_i}. \tag{11}$$

This is indeed a bijection because the Chinese remainder theorem ensures the uniqueness of  $\kappa$  in  $\mathbb{Z}_d$  such that  $\kappa \pmod{d_1} = \kappa_1$  and  $\kappa \pmod{d_2} = \kappa_2$  (and similarly for  $\lambda, \mu, \nu$ ). Furthermore,  $(1_{\mathbb{Z}_{d_1}}, 1_{\mathbb{Z}_{d_2}})$  is mapped to  $1_{\mathbb{Z}_d}$ . This gives the bijection between  $Sp(2, \mathbb{Z}_{d_1}) \times Sp(2, \mathbb{Z}_{d_2})$  and  $Sp(2, \mathbb{Z}_d)$ , and therefore  $v(d)$  is a multiplicative function. This together with equation (8) proves equation (7).  $\square$

Similar results also hold for larger matrices (see also [25]):

$$|SL(m, \mathbb{Z}_d)| = |GL(m, \mathbb{Z}_d)|/\phi(d) = d^M \prod_{k=2}^m J_k(d); \quad M = \frac{m(m-1)}{2}. \tag{12}$$

### 3. Quantum systems with positions and momenta in the ring $\mathbb{Z}_d$

We consider a quantum system where position and momentum take values in  $\mathbb{Z}_d$ , where  $d$  is an odd integer. The Hilbert space  $\mathcal{H}$  of this system is  $d$ -dimensional. The states  $|X; m\rangle$  where  $m \in \mathbb{Z}_d$  is an orthonormal basis, which we call position states. Here  $X$  is not a variable; it simply indicates position states.

The Fourier operator is defined as

$$F = d^{-1/2} \sum_{m,n \in \mathbb{Z}_d} \omega(mn) |X; m\rangle \langle X; n|; \quad \omega(k) = \exp\left(\frac{2\pi k}{d}\right); \quad F^4 = \mathbf{1}. \tag{13}$$

Acting with the Fourier operator on the position states we get another orthonormal basis:

$$|P; m\rangle = F|X; m\rangle = d^{-1/2} \sum_{n \in \mathbb{Z}_d} \omega(mn)|X; n\rangle. \quad (14)$$

We call them momentum states. Here  $P$  is not a variable but it simply indicates momentum states.

The position-momentum phase space is the toroidal lattice  $\mathbb{Z}_d \times \mathbb{Z}_d$ . Displacement operators are defined as

$$\begin{aligned} Z^\alpha &= \sum_{n \in \mathbb{Z}_d} \omega(n\alpha)|X; n\rangle\langle X; n| = \sum_{n \in \mathbb{Z}_d} |P; n + \alpha\rangle\langle P; n| \\ X^\beta &= \sum_{n \in \mathbb{Z}_d} \omega(-n\beta)|P; n\rangle\langle P; n| = \sum_{n \in \mathbb{Z}_d} |X; n + \beta\rangle\langle X; n| \end{aligned} \quad (15)$$

where  $\alpha, \beta \in \mathbb{Z}_d$ . They obey the relation

$$X^\beta Z^\alpha = Z^\alpha X^\beta \omega(-\alpha\beta); \quad X^d = Z^d = \mathbf{1}; \quad \alpha, \beta \in \mathbb{Z}_d. \quad (16)$$

General displacement operators are given by

$$\begin{aligned} D(\alpha, \beta) &= Z^\alpha X^\beta \omega(-2^{-1}\alpha\beta); \quad [D(\alpha, \beta)]^\dagger = D(-\alpha, -\beta) \\ D(\alpha_1, \beta_1)D(\alpha_2, \beta_2) &= D(\alpha_1 + \alpha_2, \beta_1 + \beta_2) \omega[2^{-1}(\alpha_1\beta_2 - \alpha_2\beta_1)]. \end{aligned} \quad (17)$$

The operators  $D(\alpha, \beta)\omega(\gamma)$  form a representation of the Heisenberg–Weyl group.

In the case of odd  $d$  which we consider here, the displacement operators obey the marginal properties [1, 18]

$$\begin{aligned} \frac{1}{d} \sum_{\beta} D(\alpha, \beta) &= |P; 2^{-1}\alpha\rangle\langle P; -2^{-1}\alpha| \\ \frac{1}{d} \sum_{\alpha} D(\alpha, \beta) &= |X; 2^{-1}\beta\rangle\langle X; -2^{-1}\beta|. \end{aligned} \quad (18)$$

### 3.1. Symplectic transformations

In this subsection we study a representation of  $Sp(2, \mathbb{Z}_d)$  in these systems. We consider the unitary transformations

$$\begin{aligned} X' &= S(\kappa, \lambda|\mu, \nu)X[S(\kappa, \lambda|\mu, \nu)]^\dagger = D(\lambda, \kappa) \\ Z' &= S(\kappa, \lambda|\mu, \nu)Z[S(\kappa, \lambda|\mu, \nu)]^\dagger = D(\nu, \mu) \\ \kappa\nu - \lambda\mu &= 1; \quad \kappa, \lambda, \mu, \nu \in \mathbb{Z}_d. \end{aligned} \quad (19)$$

The constraint ensures that these transformations preserve equations (16):

$$(X')^\beta (Z')^\alpha = (Z')^\alpha (X')^\beta \omega(-\alpha\beta); \quad (X')^d = (Z')^d = \mathbf{1}; \quad \alpha, \beta \in \mathbb{Z}_d. \quad (20)$$

These transformations form a representation of the  $Sp(2, \mathbb{Z}_d)$  group.

$S(\kappa, \lambda|\mu, \nu)$  is a unitary operator which has been given in [1, 18] for the case of a prime number  $d$  (and  $\kappa \neq 0$  and  $(1 + \lambda\mu) \neq 0$ ):

$$S(\kappa, \lambda|\mu, \nu) = S(1, 0|\xi_1, 1)S(1, \xi_2|0, 1)S(\xi_3, 0|0, \xi_3^{-1}) \quad (21)$$

where

$$\begin{aligned} S(1, 0|\xi, 1) &= \sum_m \omega(-2^{-1}\xi m^2)|P; m\rangle\langle P; m| \\ S(1, \xi|0, 1) &= \sum_m \omega(2^{-1}\xi m^2)|X; m\rangle\langle X; m| \\ S(\xi, 0|0, \xi^{-1}) &= \sum_n |X; \xi n\rangle\langle X; n| = \sum_n |P; \xi^{-1}n\rangle\langle P; n|. \end{aligned} \quad (22)$$

and

$$\begin{aligned}\xi_1 &= \mu\kappa(1 + \lambda\mu)^{-1} \\ \xi_2 &= \lambda\kappa^{-1}(1 + \lambda\mu) \\ \xi_3 &= \kappa(1 + \lambda\mu)^{-1}.\end{aligned}\tag{23}$$

In the case of a non-prime number  $d$ , equation (21) is still valid when  $\kappa \in \mathbb{Z}_d^*$  and  $(1 + \lambda\mu) \in \mathbb{Z}_d^*$  (in this case the  $\xi_1, \xi_2, \xi_3$  are well defined). For the general case, the operator  $S(\kappa, \lambda|\mu, \nu)$  has been constructed in [19].

We can prove that

$$S(\kappa, \lambda|\mu, \nu)D(\alpha, \beta)[S(\kappa, \lambda|\mu, \nu)]^\dagger = D(\alpha\nu + \beta\lambda, \alpha\mu + \beta\kappa).\tag{24}$$

The Fourier transform is a symplectic transformation

$$S(0, 1| -1, 0) = F.\tag{25}$$

Below we will use the notation

$$|X(\kappa, \lambda|\mu, \nu); n\rangle \equiv S(\kappa, \lambda|\mu, \nu)|X; n\rangle; \quad |P(\kappa, \lambda|\mu, \nu); n\rangle \equiv S(\kappa, \lambda|\mu, \nu)|P; n\rangle.\tag{26}$$

Using equation (25), we see that

$$|P(\kappa, \lambda|\mu, \nu); n\rangle = S(\kappa, \lambda|\mu, \nu)F|X; n\rangle = |X(-\lambda, \kappa, | -\nu, \mu); n\rangle.\tag{27}$$

We will also use the projectors  $\Pi(X; n) \equiv |X; n\rangle\langle X; n|$  and more generally the projectors

$$\Pi[X(\kappa, \lambda|\mu, \nu); n] \equiv S(\kappa, \lambda|\mu, \nu)\Pi(x; n)[S(\kappa, \lambda|\mu, \nu)]^\dagger.\tag{28}$$

## 4. Quantum tomography

### 4.1. Marginal properties of the displacement and parity operators

In [1, 18] we have presented Radon transforms and quantum tomography for systems where the position and momentum take values in a field. When we go from fields to rings some of the steps in this formalism (which rely on the existence of inverses) are not valid. In this section we present briefly this formalism with emphasis on the steps which are not valid in the case of a ring. We stress again that  $d$  is an odd integer (and  $2^{-1}$  exists).

The parity operator around the point  $(\alpha, \beta)$  in phase space is defined as

$$P(\alpha, \beta) = D(\alpha, \beta)F^2[D(\alpha, \beta)]^\dagger = D(2\alpha, 2\beta)F^2 = F^2[D(2\alpha, 2\beta)]^\dagger\tag{29}$$

and satisfies the relation  $[P(\alpha, \beta)]^2 = \mathbf{1}$ . It is related to the displacement operator  $D(\gamma, \delta)$  through a two-dimensional Fourier transform

$$\frac{1}{d} \sum_{\alpha, \beta} D(\alpha, \beta)\omega(\beta\gamma - \alpha\delta) = P(\gamma, \delta).\tag{30}$$

We next act with  $S(\kappa, \lambda|\mu, \nu)$  on the left-hand side and with  $[S(\kappa, \lambda|\mu, \nu)]^\dagger$  on the right-hand side of equation (18) and use equation (24). We then change variables from  $\alpha, \beta$  to  $\epsilon = \alpha\nu + \beta\lambda, \zeta = \alpha\mu + \beta\kappa$  taking into account the fact that this is a one-to-one map from  $\mathbb{Z}_d \times \mathbb{Z}_d$  to  $\mathbb{Z}_d \times \mathbb{Z}_d$  (because the matrix  $g(\nu, \lambda|\mu, \kappa)$  has an inverse). We prove that

$$\begin{aligned}\frac{1}{d} \sum_{\epsilon, \zeta} D(\epsilon, \zeta)\delta(\kappa\epsilon - \lambda\zeta, \alpha) &= |P(\kappa, \lambda|\mu, \nu); 2^{-1}\alpha\rangle\langle P(\kappa, \lambda|\mu, \nu); -2^{-1}\alpha| \\ \frac{1}{d} \sum_{\epsilon, \zeta} D(\epsilon, \zeta)\delta(-\mu\epsilon + \nu\zeta, \beta) &= |X(\kappa, \lambda|\mu, \nu); 2^{-1}\beta\rangle\langle X(\kappa, \lambda|\mu, \nu); -2^{-1}\beta|.\end{aligned}\tag{31}$$

These equations are the Radon transform for the displacement operators in our context, in the sense that we sum over all points that satisfy the linear equations  $\kappa\epsilon - \lambda\zeta = \alpha$  and  $-\mu\epsilon + \nu\zeta = \beta$ . Equation (27) shows that the two equations in (31) produce the same set of equations when the parameters vary, and for this reason below we use only one of them.

Acting with  $P(0, 0) = F^2$  on the right-hand side of equation (31), we get the Radon transform for the parity operators:

$$\frac{1}{d} \sum_{\epsilon, \zeta} P(\epsilon, \zeta) \delta(-\mu\epsilon + \nu\zeta, \beta) = \Pi[X(\kappa, \lambda|\mu, \nu); \beta]. \quad (32)$$

The Fourier transform of equations (32) using equation (30) leads to the inverse Radon transform

$$D(\nu\alpha, \mu\alpha) = \sum_{\beta} \Pi[X(\kappa, \lambda|\mu, \nu); \beta] \omega(\alpha\beta). \quad (33)$$

Quantum tomography is a direct consequence of this equation and is discussed below.

#### 4.2. Construction of the Weyl function on $\mathbb{Z}_d \times \mathbb{Z}_d$

Let  $\rho$  be the density matrix of a system with positions and momenta in  $\mathbb{Z}_d$ . It is a  $d \times d$  Hermitian matrix with trace equal to 1, and therefore it contains  $d^2 - 1$  real independent parameters. The trace of the product of  $\rho$  with the displacement operator gives the Weyl function

$$\tilde{W}(\alpha, \beta) \equiv \text{Tr}[\rho D(\alpha, \beta)]; \quad \tilde{W}(-\alpha, -\beta) = [\tilde{W}(\alpha, \beta)]^*; \quad \tilde{W}(0, 0) = 1. \quad (34)$$

The above properties of the Weyl function show that the Weyl function in the whole phase space  $\mathbb{Z}_d \times \mathbb{Z}_d$  contains  $d^2 - 1$  real independent parameters.

The trace of the product of a density matrix  $\rho$  with the parity operator gives the Wigner function

$$W(\alpha, \beta) = \text{Tr}[\rho P(\alpha, \beta)]. \quad (35)$$

The results of the previous subsection can be expressed in terms of Wigner and Weyl functions. For example equation (30) leads to the fact that the Wigner and Weyl functions are related through the Fourier transform:

$$\frac{1}{d} \sum_{\alpha, \beta} \tilde{W}(\alpha, \beta) \omega(\beta\gamma - \alpha\delta) = W(\gamma, \delta). \quad (36)$$

In a similar way equation (32) leads to the marginal properties of the Wigner function

$$\frac{1}{d} \sum_{\epsilon, \zeta} W(\epsilon, \zeta) \delta(-\mu\epsilon + \nu\zeta, \beta) = \text{Tr}\{\rho \Pi[X(\kappa, \lambda|\mu, \nu); \beta]\}, \quad (37)$$

and equation (31) leads to the marginal properties of the Weyl function

$$\frac{1}{d} \sum_{\epsilon, \zeta} \tilde{W}(\epsilon, \zeta) \delta(-\mu\epsilon + \nu\zeta, \beta) = \langle X(\kappa, \lambda|\mu, \nu); -2^{-1}\beta | \rho | X(\kappa, \lambda|\mu, \nu); 2^{-1}\beta \rangle. \quad (38)$$

Quantum tomography is based on the following equations which follow from equation (33):

$$\tilde{W}(\nu\alpha, \mu\alpha) = \sum_{\beta} \text{Tr}\{\rho \Pi[X(\kappa, \lambda|\mu, \nu); \beta]\} \omega(\alpha\beta). \quad (39)$$

This is the inverse Radon transform in the present context. The  $\text{Tr}\{\rho \Pi[X(\kappa, \lambda|\mu, \nu); \alpha]\}$  are experimentally measurable quantities and we can construct the right-hand side of

equation (39) for all values of  $\beta$  and for all values of  $(\kappa, \lambda, \mu, \nu)$  such that  $S(\kappa, \lambda|\mu, \nu)$  exists (or equivalently, such that the matrix  $g(\kappa, \lambda|\mu, \nu)$  exists).

At the origin  $(0, 0)$  we have seen that  $\tilde{W}(0, 0) = 1$  and this can also be seen through equation (39) with  $\alpha = 0$ . Below we consider points different from the origin. It is not clear if equation (39) can give the Weyl function in the whole phase space and we now prove that this is the case.

**Proposition 4.1.**

- (1) Given non-zero  $\gamma, \delta \in \mathbb{Z}_d$ , let  $\nu = \gamma/\mathfrak{G}(\gamma, \delta)$  and  $\mu = \delta/\mathfrak{G}(\gamma, \delta)$ . Then there exist exactly  $d$  matrices  $g(\kappa, \lambda|\mu, \nu)$  corresponding to these  $(\mu, \nu)$ .  $\tilde{W}(\gamma, \delta)$  can be calculated using any of these matrices and equation (39) with  $\alpha = \mathfrak{G}(\gamma, \delta)$ .
- (2) The  $\tilde{W}(\gamma, 0)$  can be calculated using equation (39) with  $\alpha = \gamma$  and any of the  $d$  matrices  $g(1, \lambda|0, 1)$ , where  $\lambda \in \mathbb{Z}_d$ .
- (3) The  $\tilde{W}(0, \delta)$  can be calculated using equation (39) with  $\alpha = \delta$  and any of the  $d$  matrices  $g(\kappa, -1|1, 0)$ , where  $\kappa \in \mathbb{Z}_d$ .

**Proof.**

- (1) We first prove that there exist at least one pair  $(\kappa, \lambda)$  such that

$$\kappa\nu - \lambda\mu = 1 \pmod{d} \tag{40}$$

$\nu, \mu$  are non-zero and coprime and therefore the inverse of  $\nu$  in  $\mathbb{Z}_\mu$  exists. This means that there exists  $\tilde{\nu}$  such that  $\nu\tilde{\nu} = 1 + N\mu$  where  $N$  is an integer. We take  $\kappa = \tilde{\nu}$  and  $\lambda = N$  and show that equation (40) is satisfied.

We now prove that there are exactly  $d$  pairs  $(\kappa, \lambda)$  corresponding to a given  $(\nu, \mu)$ . We first consider the case where at least one of the  $(\nu, \mu)$  is an invertible element. If  $\mu$  is invertible, then the  $d$  pairs have any  $\kappa \in \mathbb{Z}_d$  and  $\lambda = (\kappa\nu - 1)\mu^{-1}$ . If  $\nu$  is invertible, then the  $d$  pairs have any  $\lambda \in \mathbb{Z}_d$  and  $\kappa = (1 + \lambda\mu)\nu^{-1}$ . We next consider the case where both  $\nu, \mu$  are non-invertible elements. If  $M, N$  are integers such that  $\mu\nu(N - M) = 0 \pmod{d}$  then we also have

$$\kappa'v - \lambda'\mu = 1 \pmod{d}; \quad \kappa' = \kappa + \mu M; \quad \lambda' = \lambda + \nu N. \tag{41}$$

But the equation  $\mu\nu(N - M) = 0 \pmod{d}$  has the solutions

$$N = M + \frac{\Lambda d}{\mathfrak{G}(d, \nu\mu)} \tag{42}$$

where  $\Lambda$  is an integer. Therefore,

$$\begin{aligned} \kappa' &= \kappa + \mu M; & \lambda' &= \lambda + \nu M + \alpha \Lambda; & \alpha &= \frac{\nu d}{\mathfrak{G}(d, \nu\mu)} \\ M &= 0, 1, \dots, \frac{d}{\mathfrak{G}(d, \mu)} - 1 & N &= 0, 1, \dots, \frac{d}{\mathfrak{G}(d, \alpha)} - 1. \end{aligned} \tag{43}$$

The values of  $M, N$  are determined from the fact that  $\kappa', \lambda'$  are integers modulo  $d$ . This shows that the number of  $(\kappa', \lambda')$  pairs is

$$\frac{d}{\mathfrak{G}(d, \mu)} \frac{d}{\mathfrak{G}(d, \alpha)} = d. \tag{44}$$

Equation (44) is proved using the relation  $\mathfrak{G}(d, \nu\mu) = \mathfrak{G}(d, \nu)\mathfrak{G}(d, \mu)$  (which holds because  $\nu, \mu$  are coprime). Then

$$a\mathfrak{G}(d, \mu) = \frac{\nu d}{\mathfrak{G}(d, \nu)} \tag{45}$$



and

$$\begin{aligned} \mathfrak{G}(d, \mu)\mathfrak{G}(d, a) &= \mathfrak{G}(d\mathfrak{G}(d, \mu), a\mathfrak{G}(d, \mu)) \\ &= \mathfrak{G}\left(d\mathfrak{G}(d, \mu), \frac{vd}{\mathfrak{G}(d, v)}\right) = d\mathfrak{G}\left(\mathfrak{G}(d, \mu), \frac{v}{\mathfrak{G}(d, v)}\right) = d. \end{aligned} \quad (46)$$

The last equality is true because  $v, \mu$  are coprime.

We next show that there are no other pairs than those in equation (41). Let us assume that there exist  $\kappa''$  and  $\lambda''$  which are not of the type given in equation (41) and which satisfy the relation  $\kappa''v - \lambda''\mu = 1 \pmod{d}$ . Then

$$(\kappa'' - \kappa)v = (\lambda'' - \lambda)\mu \pmod{d}. \quad (47)$$

Since  $v, \mu$  are coprime, this implies that  $v_1$  is a divisor of  $\lambda'' - \lambda$  and  $\mu_1$  is a divisor of  $\kappa'' - \kappa$ . But this contradicts the assumption that  $\kappa''$  and  $\lambda''$  are not of the type given in equation (41). This completes the proof of the first part of the proposition.

(2) The proof here is straightforward.

(3) The proof here is straightforward. □

We have shown that there are exactly  $d$  matrices  $g(\kappa, \lambda|\mu, v)$  corresponding to the same  $(v, \mu)$ . They all give the Weyl function in the same ‘line’  $(v\alpha, \mu\alpha)$  (the set of points  $(v\alpha, \mu\alpha)$  with  $\alpha \in \mathbb{Z}_d$  and fixed  $(v, \mu)$ ). From an experimental point of view this leads to unnecessary duplication of measurements. The significance of the above proposition is to show that ‘economical tomography’ needs to use

$$\frac{|Sp(2, \mathbb{Z}_d)|}{d} = J_2(d) \quad (48)$$

lines.

## 5. Discussion

We have considered quantum systems, with positions and momenta in  $\mathbb{Z}_d$  ( $d$  is an odd integer). We have studied symplectic transformations and proved that the order of  $Sp(2, \mathbb{Z}_d)$  is given in equation (7). These transformations have been used in the context of quantum tomography. We have shown that equation (39) gives the Weyl function and that for ‘economical tomography’ it needs to be used on  $J_2(d)$  lines.

We note that there are factorizations of finite systems in terms of subsystems [26, 27]. Such factorizations have been used extensively in fast Fourier transforms. The use of tomography techniques on the various subsystems is an interesting problem for further work. We also point out that in a classical tomography context, there is much work on ‘discrete tomography’ [28].

## Acknowledgments

Helpful discussions with P Blasiak, G H E Duchamp, P Flajolet, A Horzela, A Orłowski, K Penson and A Solomon, during the workshop on ‘Quantum and Combinatorics’, in Poland 2009, are gratefully acknowledged.

## References

- [1] Vourdas A 2004 *Rep. Prog. Phys.* **67** 1  
Vourdas A 2007 *J. Phys. A: Math. Theor.* **40** R285
- [2] Kibler M 2009 *J. Phys. A: Math. Gen.* **42** 353001

- [3] Bjork G, Klimov A B and Sanchez-Soto L L 2008 *Prog. Opt.* **51** 469
- [4] Berndt B C, Evans R J and Williams K S 1998 *Gauss and Jacobi Sums* (New York: Wiley)
- [5] Terras A 1999 *Fourier Analysis on Finite Groups and Applications* (London: London Mathematical Society)
- [6] Weil A 1964 *Acta Math.* **111** 143  
Weil A 1965 *Acta Math.* **113** 1
- [7] Auslander L and Tolimieri R 1979 *Bull. Am. Math. Soc.* **1** 847
- [8] Ivanovic I D 1981 *J. Phys. A: Math. Gen.* **14** 3421
- [9] Wootters W and Fields B D 1989 *Ann. Phys., NY* **191** 363  
Gibbons K, Hoffman M J and Wootters W 2004 *Phys. Rev. A* **70** 062101
- [10] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512
- [11] Chaturvedi S 2002 *Phys. Rev. A* **65** 044301
- [12] Klimov A, Sanchez-Soto L and de Guise H 2005 *J. Phys. A: Math. Gen.* **38** 2747  
Romero J L, Bjork G, Klimov A B and Sanchez-Soto L L 2005 *Phys. Rev. A* **72** 062310  
Bjork G, Romero J L, Klimov A B and Sanchez-Soto L L 2007 *J. Opt. Soc. Am. B* **24** 371
- [13] Saniga M and Planat M 2006 *J. Phys. A: Math. Gen.* **39** 435  
Kibler M R and Planat M 2006 *Int. J. Mod. Phys. B* **20** 1802
- [14] Klappenecker A and Rotteler M 2004 *Lect. Notes Comp. Sci.* **2948** 137  
Pittenger A O and Rubin M H 2004 *Linear Algebra Appl.* **390** 255  
Archer C 2005 *J. Math. Phys.* **46** 022106
- [15] Sulc P and Tolar J 2007 *J. Phys. A: Math. Theor.* **40** 15099  
Tolar J and Chadzitaskos G 2009 *J. Phys. A: Math. Theor.* **42** 245306
- [16] Piatetskii-Shapiro I I 1983 *Complex Representations of  $GL(2, K)$  for Finite Fields  $K$*  (Providence: American Mathematical Society)
- [17] Vourdas A 1991 *Phys. Rev. A* **43** 1564
- [18] Vourdas A 2005 *J. Phys. A: Math. Gen.* **38** 8453  
Vourdas A 2006 *J. Math. Phys.* **47** 092104  
Vourdas A 2008 *J. Fourier Anal. Appl.* **14** 102
- [19] Feichtinger H G, Hazewinkel M, Kaiblinger N, Matusiak E and Neuhauser M 2008 *Quartely J. Math.* **59** 15
- [20] Luis A and Perina J 1998 *J. Phys. A: Math. Gen.* **31** 1423
- [21] Pittenger A O and Rubin M H 2005 *J. Phys. A: Math. Gen.* **38** 6005
- [22] Miquel C, Paz J P, Saraceno M, Knill M, Laflamme R and Negrevergne C 2002 *Nature* **418** 59  
Cormick C, Calvao E F, Gottesman D, Paz J P and Pittenger A O 2006 *Phys. Rev. A* **73** 012301
- [23] Klimov A B, Munoz C and Romero J L 2006 *J. Phys. A: Math. Gen.* **39** 14471
- [24] Vourdas A 1996 *J. Phys. A: Math. Gen.* **29** 4275  
Vourdas A 1997 *Rep. Math. Phys.* **40** 367  
Al Hadhrami H and Vourdas A 2009 *Phys. Rev. A* **80** 022110
- [25] Overbey J, Traves W and Wojdylo J 2005 *Cryptologia* **29** 59  
Schulte J 1999 *Resultate der Mathematik* **36** 354
- [26] Vourdas A and Bendjaballah C 1993 *Phys. Rev. A* **47** 3523  
Vourdas A 2003 *J. Phys. A: Math. Gen.* **36** 5645
- [27] Mann A, Revzen M and Zak J 2005 *J. Phys. A: Math. Gen.* **38** L389  
Revzen M, Khanna F C, Mann A and Zak J 2006 *J. Phys. A: Math. Gen.* **39** 5151  
Mann A, Revzen M and Zak J 2008 *Europhys. Lett.* **83** 10007
- [28] Herman G T and Kuba A (eds) 1999 *Discrete Tomography: Foundations, Algorithms and Applications* (Boston: Birkhauser)