published in J. Phys. A43 (2010) 042001

Symplectic transformations and quantum tomography in finite quantum systems

A. Vourdas [(1)] and C. Banderier[(2)]
[(1)] Department of Computing,
University of Bradford,
Bradford BD7 1DP, United Kingdom
[(2)]Laboratoire d'informatique de Paris-Nord, UMR CNRS 7030,
Université Paris XIII,
Villetaneuse, France

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).

I. 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 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 that $\mathbb{Z}_d$ 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 paper 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 II.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 IV.1. We conclude in section 5 with a discussion of our results.

A. 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 $N = 0, 1, ..., p^{e-1} - 1$. 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 ψ-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).

II. 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

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

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 $g(\nu, -\lambda | -\mu, \kappa)$. Therefore these matrices form a group which is the $Sp(2, \mathbb{Z}_d)$ group.

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

$$|Sp(2, \mathbb{Z}_d)| = d J_2(d). \tag{7}$$

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-overlaping subsets of $Sp(2,\mathbb{Z}_d)$ (where $\kappa \in \mathbb{Z}_d^*$, and $\kappa = Np$) and their cardinalities:

$$\begin{aligned}
\mathcal{S}_1 &= \{g(\kappa,\lambda|\mu,\kappa^{-1}(1+\lambda\mu)) \mid \kappa \in \mathbb{Z}_{p^e}^*;\ \ \lambda,\mu\in\mathbb{Z}_d\}; \quad |\mathcal{S}_1| = d^2\varphi(d)\\
\mathcal{S}_2 &= \{g(Np,\lambda|\mu,\nu)\ |N=0,1,...,\frac{d}{p}-1; \quad \lambda,\mu\in\mathbb{Z}_d^*;\ \ \nu\in\mathbb{Z}_d\}; \quad |\mathcal{S}_2| = d^2\varphi(d)\frac{1}{p}.
\end{aligned} \tag{9}$$

In $\mathcal{S}_2$ we have $\lambda\mu = Np\nu - 1$ and this shows that λ,μ are invertible elements and therefore $|\mathcal{S}_2| = d^2\varphi(d)\frac{1}{p}$. Adding these two cardinalities we prove Eq.(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

$$\kappa_i = \kappa(\text{mod } d_i); \quad \lambda_i = \lambda(\text{mod } d_i); \quad \mu_i = \mu(\text{mod } d_i); \quad \nu_i = \nu(\text{mod } d_i). \tag{11}$$

This is indeed a bijection because the the Chinese reminder theorem ensures the uniqueness of κ in $\mathbb{Z}_d$ such that $\kappa(\text{mod } \mathrm{d}_1) = \kappa_1$ and $\kappa(\text{mod } \mathrm{d}_2) = \kappa_2$ (and similarly for λ,μ,ν). 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 Eq.(8) prove Eq.(7). □

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

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

III. 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:

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

. We call them mommentum 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

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

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

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

General displacement operators are given by

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

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]

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

A. Symplectic transformations

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

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

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

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

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 refs[1, 18] for the case of a prime number d (and $\kappa \neq 0$ and $(1+\lambda\mu) \neq 0$):

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

where

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

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, Eq.(21) is still valid when $\kappa \in \mathbb{Z}_d^*$ and $(1+\lambda\mu) \in \mathbb{Z}_d^*$ (in this case the ξ_1, ξ_2, ξ_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

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

Using Eq.(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

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

IV. QUANTUM TOMOGRAPHY

A. Marginal properties of the displacement and parity operators

In refs[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 the 2^{-1} exists).

The parity operator around the point (α, β) 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 Eq.(18) and use Eq.(24). We then change variables from α, β 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 $-\mu\epsilon + \nu\zeta = \beta$. Eq.(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 Eq.(31), we get the Radon transform for the parity operators:

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

The Fourier transform of Eqs.(32) using Eq.(30) leads to the inverse Radon transform

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

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

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

Let ρ 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 ρ with the displacement operator gives the Weyl function

$$\widetilde{W}(\alpha,\beta) \equiv \mathrm{Tr}[\rho D(\alpha,\beta)]; \qquad \widetilde{W}(-\alpha,-\beta) = [\widetilde{W}(\alpha,\beta)]^*; \qquad \widetilde{W}(0,0) = 1. \tag{34}$$

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 ρ with the parity operator gives the Wigner function

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

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

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

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

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

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

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

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

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

This is the inverse Radon transform in the present context. The $\mathrm{Tr}\{\rho\;\Pi[X(\kappa,\lambda|\mu,\nu);\alpha]\}$ are experimentaly measurable quantities and we can construct the right hand side of Eq.(39) for all values of β and for all values of (κ,λ,μ,ν) such that the $S(\kappa,\lambda|\mu,\nu)$ exists (or equivalently, such that the matrix $g(\kappa,\lambda|\mu,\nu)$ exists).

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

Proposition IV.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 exists exactly d matrices $g(\kappa,\lambda|\mu,\nu)$ corresponding to these (μ,ν). $\widetilde{W}(\gamma,\delta)$ can be calculated using any of these matrices and Eq.(39) with $\alpha=\mathfrak{G}(\gamma,\delta)$.

(2) The $\widetilde{W}(\gamma,0)$ can be calculated using Eq.(39) with $\alpha=\gamma$ and any of the d matrices $g(1,\lambda|0,1)$, where $\lambda\in\mathbb{Z}_d$.

(3) The $\widetilde{W}(0,\delta)$ can be calculated using Eq.(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 exists at least one pair (κ,λ) such that

$$\kappa\nu-\lambda\mu=1\;(\mathrm{mod}\;d) \tag{40}$$

The ν,μ are non-zero and coprime and therefore the inverse of ν 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 Eq.(40) is satisfied.

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

$$\kappa'\nu-\lambda'\mu=1\;(\mathrm{mod}\;d);\qquad \kappa'=\kappa+\mu M;\qquad \lambda'=\lambda+\nu N \tag{41}$$

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

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

where Λ is an integer. Therefore

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

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

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

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

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

and

$$\mathfrak{G}(d,\mu)\mathfrak{G}(d,a) = \mathfrak{G}(d\mathfrak{G}(d,\mu), a\mathfrak{G}(d,\mu)) = \mathfrak{G}\left(d\mathfrak{G}(d,\mu), \frac{\nu d}{\mathfrak{G}(d,\nu)}\right) = d\mathfrak{G}\left(\mathfrak{G}(d,\mu), \frac{\nu}{\mathfrak{G}(d,\nu)}\right) = d. \tag{46}$$

The last equality is true because ν, μ are coprime.

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

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

Since ν, μ are coprime, this implies that ν_1 is a divisor of $\lambda'' - \lambda$ and μ_1 is a divisor of $\kappa'' - \kappa$. But this contradicts the assumption that κ'' and λ'' are not of the type given in Eq.(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 $g(\kappa, \lambda|\mu, \nu)$ corresponding to the same (ν, μ). They all give the Weyl function in the same 'line' $(\nu\alpha, \mu\alpha)$. (the set of points $(\nu\alpha, \mu\alpha)$ with $\alpha \in \mathbb{Z}_d$ and fixed (ν, μ)). 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

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

lines.

V. 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 Eq.(7). These transformations have been used in the context of quantum tomography. We have shown that Eq.(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].

VI. ACKNOWLEDGEMENT

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

[1] A. Vourdas, Rep. Prog. Phys. 67, 1 (2004)
A. Vourdas, J. Phys. A40, R285 (2007)
[2] M. Kibler, J. Phys. A42, 353001 (2009)
[3] G. Bjork, A.B. Klimov, L.L. Sanchez-Soto, Prog. Optics 51, 469 (2008)
[4] B.C. Berndt, R.J. Evans, K.S. Williams, 'Gauss and Jacobi sums' (Wiley, New York, 1998)
[5] A. Terras, 'Fourier analysis on finite groups and applications' (London Math. Soc. London, 1999)
[6] A. Weil Acta Math. 111, 143 (1964)
A. Weil Acta Math. 113, 1 (1965)
[7] L. Auslander, R. Tolimieri, Bull. Am. Math. Soc. 1, 847 (1979)
[8] I.D. Ivanovic, J. Phys. A14, 3421 (1981)
[9] W. Wootters, B.D. Fields, Ann. Phys. (NY), 191, 363 (1989)
K. Gibbons, M.J. Hoffman, W. Wootters, Phys. Rev. A70, 062101 (2004)
[10] S. Bandyopadhyay, P.O. Boykin, V.Roychowdhury, F. Vatan, Algorithmica 34, 512 (2002)
[11] S. Chaturvedi, Phys. Rev. A65, 044301 (2002)
[12] A. Klimov, L. Sanchez-Soto, H. de Guise, J. Phys. A38, 2747 (2005)
J.L. Romero, G. Bjork, A.B. Klimov, L.L. Sanchez-Soto, Phys. Rev. A72, 062310 (2005)
G. Bjork, J.L. Romero, A.B. Klimov, L.L. Sanchez-Soto, J. Opt. Soc. Amer. B24, 371 (2007)
[13] M. Saniga, M. Planat, J. Phys. A39, 435 (2006)
M.R. Kibler, M. Planat, Intern. J. Mod. Phys. B20, 1802 (2006)
[14] A. Klappenecker, M. Rotteler, Lect. Notes Comp. Science 2948, 137 (2004)
A.O. Pittenger, M.H. Rubin, Linear Algebra Appl. 390, 255 (2004)
C. Archer, J. Math. Phys. 46, 022106 (2005)
[15] P. Sulc, J. Tolar, J. Phys. A40, 15099 (2007)
J. Tolar, G. Chadzitaskos, J. Phys. A42, 245306 (2009)
[16] I.I. Piatetskii-Shapiro, 'Complex Representations of $GL(2,K)$ for finite fields K' (Amer. Math. Soc. Providence, 1983
[17] A. Vourdas, Phys. Rev. A43, 1564 (1991)
[18] A. Vourdas, J.Phys.A38, 8453 (2005)
A. Vourdas, J. Math. Phys. 47, 092104 (2006)
A. Vourdas, J. Fourier Anal. Appl. 14, 102 (2008)
[19] H.G. Feichtinger, M. Hazewinkel, N. Kaiblinger, E. Matusiak, M. Neuhauser, Quartely J. Math.,59, 15 (2008)
[20] A. Luis, J. Perina, J. Phys. A31, 1423 (1998)

[21] A.O. Pittenger, M.H. Rubin, J. Phys. A38, 6005 (2005)
[22] C. Miquel, J.P. Paz, M. Saraceno, M. Knill, R. Laflamme, C. Negreverdne, Nature 418, 59 (2002)
C. Cormick, E.F. Calvao, D. Gottesman, J.P. Paz, A.O. Pittenger, Phys. Rev. A73, 012301 (2006)
[23] A.B. Klimov, C. Munoz, J.L. Romero, J. Phys. A39, 14471 (2006)
[24] A. Vourdas, J. Phys. A29, 4275 (1996)
A. Vourdas, Rep. Math. Phys. 40, 367 (1997)
H. Al Hadhrami, A. Vourdas, Phys. Rev. A80, 022110 (2009)
[25] J. Overbey, W. Traves, J. Wojdylo, Cryptologia. 29(1), 59, (2005)
J. Schulte, Resultate der Mathematik, 36, 354 (1999)
[26] A. Vourdas, C. Bendjaballah, Phys. Rev. A47, 3523 (1993)
A. Vourdas, J. Phys. A36, 5645 (2003)
[27] A. Mann, M. Revzen, J. Zak, J. Phys. A38, L389 (2005)
M. Revzen, F.C. Khanna, A. Mann, J. Zak, J. Phys. A39, 5151 (2006)
A. Mann, M. Revzen, J. Zak, Europhys. Lett. 83, 10007 (2008)
[28] G.T. Herman, A. Kuba (Eds), 'Discrete tomography: foundations, algorithms and applications', (Birkhauser, Boston, 1999)