Geometrical approach to the discrete Wigner function in prime power dimensions

2006 J. Phys. A: Math. Gen. 39 14471

(http://iopscience.iop.org/0305-4470/39/46/016)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **39** (2006) 14471–14497 doi:10.1088/0305-4470/39/46/016

Geometrical approach to the discrete Wigner function in prime power dimensions

A B Klimov, C Muñoz and J L Romero

Departamento de Física, Universidad de Guadalajara, Revolución 1500, 44410, Guadalajara, Jal., Mexico

Received 15 May 2006, in final form 6 October 2006
Published 1 November 2006
Online at stacks.iop.org/JPhysA/39/14471

Abstract
We analyse the Wigner function in prime power dimensions constructed on the basis of the discrete rotation and displacement operators labelled with elements of the underlying finite field. We separately discuss the case of odd and even characteristics and analyse the algebraic origin of the non-uniqueness of the representation of the Wigner function. Explicit expressions for the Wigner kernel are given in both cases.

PACS numbers: 03.67.−a, 03.65.Ca

1. Introduction

Wootters' construction of the Wigner function [1, 2] in the discrete phase space for quantum systems whose dimension $d = p^n$ is a power of a prime number has been applied for the analysis of several problems, mainly related to quantum information processes [3–6]. In this case, the phase space is a $d \times d$ grid with a well-defined geometrical structure (the so-called finite geometry) [7], which is a direct consequence of the underlying finite field (Galois field) structure, so that the phase-space coordinates can be chosen as elements of the corresponding finite field [1, 2]. The Wigner function (a discrete symbol of the density matrix) is constructed using the so-called phase point operators and consists of a highly non-unique procedure of association of states in the Hilbert space with some geometrical structures (lines) in the discrete phase space.

Slightly different, operational approaches to the Wigner function construction, based on the algebraic structure of the Galois fields, have been recently [8–11] proposed for the quantum systems of prime power dimensions, although for the prime dimensions such constructions were also discussed earlier [13, 14].

In the present paper we analyse the Wigner function constructed on the basis of the discrete rotation and displacement operators labelled with the elements of the underlying finite field. We separately discuss the case of odd and even characteristics and analyse the algebraic origin of the non-uniqueness of the representation of the Wigner function in both cases. The main difference with Wootters' method consists of labelling the elements of the Hilbert space and the operators acting on this space directly by the elements of the finite field [12], so that the possible factorizations of the corresponding operators appear as a result of choosing a different basis in the field, and are not really necessary for the phase space construction.

The paper is organized as follows. In section 2 we outline the structure of the generalized Pauli group and introduce the Wigner mapping as that which satisfies the Stratonovich–Weyl postulates and shows the phase problem for the displacement operator. In section 3 we analyse the rotation operators for fields of odd and even characteristics and discuss the discrete phase space construction. In section 4 we briefly outline the reconstruction procedure. In section 5 we discuss different possibilities for ordering points in the phase space with elements of the finite field. In section 6 we analyse the relation between abstract states and states of physical systems. Several useful relations are proved in the appendices.

2. General definitions

In the case of prime power dimensions, $d = p^n$, the phase-space representation can be constructed in a similar way as in the prime dimensions [1, 13]. We perform the Wigner mapping in a slightly different manner than in [2], by using the generalized position and momentum operators introduced in [12] (see also [8]). In the case of composite dimensions instead of natural numbers we have to use the elements of the finite field $GF(d)$ to label the states of the system and operators acting on the corresponding Hilbert space. In particular, we will denote as $|\alpha\rangle, \alpha \in GF(d)$ (in the case of $\mathcal{Z}_p$ we shall use Latin characters, instead) an orthonormal basis in the Hilbert space of the quantum system, $\langle\alpha|\beta\rangle = \delta_{\alpha,\beta}$. Operationally, the elements of the basis can be labelled by powers of primitive elements (see appendix A). These vectors will be considered as eigenvectors of the generalized position operator which belong to the generalized Pauli group. The generators of this group, usually called generalized position and momentum operators, are defined as follows,

$$Z_\beta|\alpha\rangle = \chi(\alpha\beta)|\alpha\rangle, \qquad X_\beta|\alpha\rangle = |\alpha+\beta\rangle, \qquad \alpha,\beta \in GF(d), \tag{1}$$

$$Z_\beta^\dagger = Z_{-\beta}, \qquad X_\beta^\dagger = X_{-\beta}, \tag{2}$$

so that

$$Z_\alpha X_\beta = \chi(\alpha\beta) X_\beta Z_\alpha,$$

where $\chi(\theta)$ is an additive character [7]

$$\chi(\theta) = \exp\left[\frac{2\pi \mathrm{i}}{p}\,\mathrm{tr}(\theta)\right], \tag{3}$$

and the trace operation, which maps the elements of $GF(d)$ into the prime field $GF(p) \simeq \mathcal{Z}_p$, is defined as

$$\mathrm{tr}(\theta) = \theta + \theta^p + \theta^{p^2} + \cdots + \theta^{p^{n-1}}.$$

This operation leaves the elements of the prime field (see appendix A) invariant. The characters (3) satisfy the following important properties,

$$\sum_{\alpha\in GF(d)} \chi(\alpha\beta) = \mathrm{d}\delta_{0,\beta}, \qquad \chi(\alpha+\beta) = \chi(\alpha)\chi(\beta), \tag{4}$$

similar to the well-known identities in the prime case

$$\sum_{m=0}^{p-1} \omega^{mn} = p\delta_{n,0}, \qquad \omega^{m+n} = \omega^m\omega^n,$$

where $\omega = \exp[2\pi\mathrm{i}/p]$ is a root of unity.

In particular, for the prime dimensional case ($d = p$), the position and momentum operators act in the standard basis $|n\rangle$, $n = 0, \ldots, p-1$, as follows [15]:

$$Z|n\rangle = \omega^n|n\rangle, \qquad X|n\rangle = |n+1\rangle, \qquad ZX = \omega XZ, \tag{5}$$

where all the algebraic operations are on $\mathrm{mod}(p)$, $n \in \mathcal{Z}_p$, and the rest of the operators, analogous to Z_α and X_β, can be obtained as powers of Z and X.

It is worth noting that there is a single element of this basis (sometimes called *stabilizer state)*, labelled with the zero element of the field, which is a common eigenstate of all Z_β with all the eigenvalues equal to unity:

$$Z_\beta|0\rangle = |0\rangle,$$

for any $\beta \in GF(d)$.

The operators (1) are related through the finite Fourier transform operator [12]

$$F = \frac{1}{\sqrt{d}} \sum_{\alpha,\beta \in GF(d)} \chi(\alpha\beta)|\alpha\rangle\langle\beta|, \qquad FF^\dagger = F^\dagger F = I, \tag{6}$$

so that

$$FX_\alpha F^\dagger = Z_\alpha, \tag{7}$$

and $F^4 = I$ for $d = p^n$ where $p \neq 2$, and $F^2 = I$ for $d = 2^n$. The Fourier transform offers us the possibility of introducing the *conjugate* basis, which is related to the basis $|\alpha\rangle$ as follows,

$$|\widetilde{\alpha}\rangle = F|\alpha\rangle, \qquad Z_\beta|\widetilde{\alpha}\rangle = |\widetilde{\alpha+\beta}\rangle, \qquad X_\beta|\widetilde{\alpha}\rangle = \chi^*(\alpha\beta)|\widetilde{\alpha}\rangle, \tag{8}$$

so that the elements of the conjugate basis are eigenvectors of the momentum operators.

The operators Z_α and X_β are particular cases of the so-called *displacement operators* which, in general, have the form

$$D(\alpha,\beta) = \phi(\alpha,\beta)Z_\alpha X_\beta, \tag{9}$$

and the phase factor $\phi(\alpha,\beta)$ is such that the unitary condition,

$$D(\alpha,\beta)D^\dagger(\alpha,\beta) = I,$$

is satisfied, implying that

$$\phi(\alpha,\beta)\phi^*(\alpha,\beta) = 1. \tag{10}$$

The operational basis (9) becomes orthogonal,

$$\mathrm{Tr}[D(\alpha_1,\beta_1)D(\alpha_2,\beta_2)] = \mathrm{d}\delta_{-\alpha_1,\alpha_2}\delta_{-\beta_1,\beta_2},$$

where Tr means the operational trace in the Hilbert space, or equivalently $D^\dagger(\alpha,\beta) = D(-\alpha,-\beta)$, if the phase $\phi(\alpha,\beta)$ satisfies the following condition,

$$\phi(\alpha,\beta)\phi(-\alpha,-\beta) = \chi(-\alpha\beta), \tag{11}$$

and for the particular case of the fields of even characteristic, char $(GF(d)) = 2$, implies that

$$\phi^2(\alpha,\beta) = \chi(\alpha\beta), \tag{12}$$

which is equivalent to $D^\dagger(\alpha,\beta) = D(\alpha,\beta)$.

In general, the displacement operators are non-Hermitian and thus cannot be used for mapping Hermitian operators into real phase-space functions. Nevertheless, a desirable Hermitian kernel can be defined as the following transformation [8, 10] of the displacement operator (9):

$$\Delta(\alpha,\beta) = \frac{1}{d} \sum_{\kappa,\lambda \in GF(d)} \chi(\alpha\lambda - \beta\kappa)D(\kappa,\lambda). \tag{13}$$

This operator can be used for mapping operators into phase-space functions in a self-consistent way and satisfies the Stratonovich–Weyl postulates [16]:

$$\textit{hermiticity}: \quad \Delta(\alpha,\beta) = \Delta^{\dagger}(\alpha,\beta), \tag{14}$$

if condition (11) (or (12) in the case $p = 2$) is satisfied;

$$\textit{normalization}: \quad \frac{1}{d}\sum_{\alpha,\beta\in GF(d)} \Delta(\alpha,\beta) = I;$$

$$\textit{covariance}: \quad D(\kappa,\lambda)\Delta(\alpha,\beta)D^{\dagger}(\kappa,\lambda) = \Delta(\alpha+\kappa,\beta+\lambda);$$

and the

$$\textit{orthogonality relation}: \quad \mathrm{Tr}(\Delta(\alpha,\beta)\Delta^{\dagger}(\alpha',\beta')) = \mathrm{d}\delta_{\alpha,\alpha'}\delta_{\beta,\beta'}.$$

Since the Stratonovich–Weyl postulates are satisfied, the symbol of an operator f is defined in the standard way,

$$W_f(\alpha,\beta) = \mathrm{Tr}[f\Delta(\alpha,\beta)], \tag{15}$$

and the inversion relation is

$$f = \frac{1}{d}\sum_{\alpha,\beta\in GF(d)} W_f(\alpha,\beta)\Delta(\alpha,\beta).$$

The *overlap relation* has the standard form

$$\mathrm{Tr}(fg) = \mathrm{d}\sum_{\alpha,\beta\in GF(d)} W_f(\alpha,\beta)W_g(\alpha,\beta),$$

and, as a particular case, the average value of the operator f is calculated as

$$\langle f\rangle = \mathrm{d}\sum_{\alpha,\beta\in GF(d)} W_f(\alpha,\beta)W_\rho(\alpha,\beta),$$

where ρ is the density matrix.

In terms of the expansion coefficients of the operator f in the operational basis (9)

$$f = \sum_{\alpha,\beta\in GF(d)} f_{\alpha,\beta}D(\alpha,\beta), \tag{16}$$

the symbol of f has the form

$$W_f(\alpha,\beta) = \sum_{\kappa,\lambda\in GF(d)} f_{\kappa,\lambda}\chi^{*}(\alpha\lambda-\beta\kappa). \tag{17}$$

As some simple examples, we obtain that the symbols of the operators Z_κ and X_λ are

$$W_{Z_\kappa}(\alpha,\beta) = \chi(\beta\kappa), \qquad W_{X_\lambda}(\alpha,\beta) = \chi(-\alpha\lambda), \tag{18}$$

and in the particular case of prime dimensions we get for the symbols of (5),

$$W_Z(a,b) = \omega^{b}, \qquad W_X(a,b) = \omega^{-a},$$

where $a, b \in \mathcal{Z}_p$. In the same way, the symbols of the basis states $|\kappa\rangle$ and $|\widetilde{\kappa}\rangle$ are

$$W_{|\kappa\rangle\langle\kappa|}(\alpha,\beta) = \delta_{\beta,\kappa}, \qquad W_{|\widetilde{\kappa}\rangle\langle\widetilde{\kappa}|}(\alpha,\beta) = \delta_{\alpha,\kappa}.$$

3. Discrete phase space construction

3.1. Lines and rays

In the discrete space $GF(d) \times GF(d)$ the concept of line can be introduced in a similar way as in the continuous plane case, so all the points $(\alpha, \beta) \in GF(d) \times GF(d)$ which satisfy the relation

$$\zeta\alpha + \eta\beta = \vartheta,$$

where ζ, η, θ are some fixed elements of $GF(d)$, form a line. Moreover, two lines,

$$\zeta\alpha + \eta\beta = \vartheta, \qquad \zeta'\alpha + \eta'\beta = \vartheta', \tag{19}$$

are called parallel if they have no common points, which implies that $\eta\zeta' = \zeta\eta'$. If the lines (19) are not parallel they cross each other at a single point with the coordinates

$$\alpha = (\eta\vartheta' - \eta'\vartheta)(\zeta'\eta - \zeta\eta')^{-1}, \qquad \beta = (\zeta\vartheta' - \zeta'\vartheta)(\zeta\eta' - \zeta'\eta)^{-1}.$$

A line which passes through the origin is called a *ray* and its equation has the form

$$\alpha = 0, \qquad \text{or} \qquad \beta = \mu\alpha \tag{20}$$

so that $\alpha = 0$ and $\beta = 0$ are the vertical and horizontal axes, correspondingly.

Each ray is characterized by the value of the 'slope' μ and we denote by λ_μ the ray which is a collection of points satisfying $\beta = \mu\alpha$ and by λ_∞ the ray corresponding to the vertical axis.

There are $d - 1$ parallel lines to each of $d + 1$ rays, so that the total number of lines is $d(d + 1)$. The collection of d parallel lines is called a *striation* [2].

3.2. Displacement operators

The displacement operators labelled with points of the phase space belonging to the same ray commute (here we omit the phase factor):

$$Z_{\alpha_1}X_{\beta_1=\mu\alpha_1}Z_{\alpha_2}X_{\beta_2=\mu\alpha_2} = \chi(-\mu\alpha_1\alpha_2)Z_{\alpha_1+\alpha_2}X_{\mu(\alpha_1+\alpha_2)} = Z_{\alpha_2}X_{\beta_2=\mu\alpha_2}Z_{\alpha_1}X_{\beta_1=\mu\alpha_1},$$

and thus have a common system of eigenvectors $\{|\psi_\nu^\mu\rangle, \mu, \nu \in GF(d)\}$:

$$Z_\alpha X_{\mu\alpha}|\psi_\nu^\mu\rangle = \exp(\mathrm{i}\xi_{\mu,\nu})|\psi_\nu^\mu\rangle, \tag{21}$$

where μ is fixed and $\exp(\mathrm{i}\xi_{\mu,\nu})$ is the corresponding eigenvalue, so that $|\psi_\nu^0\rangle \equiv |\nu\rangle$ are eigenstates of the Z_α operators (displacement operators labelled with the points of the ray $\beta = 0$ horizontal axis) and $|\tilde{\psi}_\nu^0\rangle = F|\psi_\nu^0\rangle \equiv |\tilde{\nu}\rangle$ are the eigenstates of the X_β operators (displacement operators labelled with the points of the ray $\alpha = 0$ vertical axis).

In the simplest cases, $d = 3$ and $d = 4$, the rays are drawn in tables 1 and 2, and the corresponding displacement operators have the form (up to a phase)

$d = 3$ ray equation	displacement operators	$d = 4$ ray equation	displacement operators
$b = 0$	Z, Z^2	$\beta = 0$	$Z_\sigma, Z_{\sigma^2}, Z_{\sigma^3}$
$b = a$	ZX, Z^2X^2	$\beta = \alpha$	$Z_\sigma X_\sigma, Z_{\sigma^2}X_{\sigma^2}, Z_{\sigma^3}X_{\sigma^3}$
$b = 2a$	$ZX^2, Z^2X^4 = Z^2X$	$\beta = \sigma\alpha$	$Z_\sigma X_{\sigma^2}, Z_{\sigma^2}X_{\sigma^3}, Z_{\sigma^3}X_\sigma$
$a = 0$	X, X^2	$\beta = \sigma^2\alpha$	$Z_\sigma X_{\sigma^3}, Z_{\sigma^2}X_\sigma, Z_{\sigma^3}X_{\sigma^2}$
		$\alpha = 0$	$X_\sigma, X_{\sigma^2}, X_{\sigma^3}$

where σ is the primitive element, a root of the polynomial $\sigma^2 + \sigma + 1 = 0$.

Table 1. The four possible rays in the $d = 3$ case. The axes are labelled by natural numbers 0, 1, 2. The points of each ray are labelled by the value of the corresponding slope, so that the vertical axis (the ray $\alpha = 0$) is labelled as ∞.

2	∞	2	1
1	∞	1	2
0		0	0
	0	1	2

Table 2. The five possible rays in the $d = 4$ case. The axes are labelled by powers of the primitive element σ. The points of each ray are labelled by the value of the corresponding slope: $\sigma, \sigma^2, \sigma^3$.

σ^3	∞	σ^2	σ	σ^3
σ^2	∞	σ	σ^3	σ^2
σ	∞	σ^3	σ^2	σ
0		0	0	0
	0	σ	σ^2	σ^3

It is easy to observe that an arbitrary displacement operator $Z_\tau X_\upsilon$ acting on an eigenstate of the set $\{Z_\alpha X_{\mu\alpha}, \mu \text{ is fixed}, \alpha \in GF(d)\}$ transforms it into another eigenstate of the same set:

$$Z_\alpha X_{\mu\alpha}\left[Z_\tau X_\upsilon\left|\psi_\nu^\mu\right\rangle\right] = \exp(\mathrm{i}\xi_{\mu,\nu})\chi(\alpha\upsilon - \mu\alpha\tau)Z_\tau X_\upsilon\left|\psi_\nu^\mu\right\rangle.$$

It is clear that if $\upsilon = \mu\tau$ we do not generate another state (in other words we do not change the index ν). Because for an arbitrary υ one can always find such $\varkappa$ that $\upsilon = \mu\tau + \varkappa$, we can generate all the states from the set $\{\left|\psi_0^\mu\right\rangle, \mu \text{ is fixed}\}$ by applying only the momentum operators X_υ (where υ runs through the whole field) to any particular state belonging to this set. It is clear that all the eigenstates of X_β operator can be obtained by applying the Z_α operator to any particular state from the set $\left\{\left|\tilde{\psi}_0^\mu\right\rangle\right\}$.

3.3. Rotation operators

The 'rotation' operators $V_{\mu'}$ which transform eigenstates of the operators associated with the ray $\beta = \mu\alpha$

$$\left\{I, Z_{\alpha_1}X_{\mu\alpha_1}, Z_{\alpha_2}X_{\mu\alpha_2}, \ldots\right\} \tag{22}$$

into eigenstates of the operators labelled with points of the ray $\beta = (\mu + \mu')\alpha$,

$$\left\{I, Z_{\alpha_1}X_{(\mu+\mu')\alpha_1}, Z_{\alpha_2}X_{(\mu+\mu')\alpha_2}, \ldots\right\}, \tag{23}$$

are defined through the relations

$$V_\mu Z_\alpha V_\mu^\dagger = \exp(\mathrm{i}\varphi(\alpha, \mu))Z_\alpha X_{\mu\alpha}, \qquad [V_\mu, X_\nu] = 0, \qquad V_0 = I, \tag{24}$$

for all $\mu, \nu \in GF(d)$.

In fact, $\left|\psi_\nu^\mu\right\rangle$ (21) being a state assigned to the ray $\beta = \mu\alpha$, we obtain after simple algebra

$$\begin{aligned} V_{\mu'}Z_\alpha X_{\mu\alpha}\left|\psi_\nu^\mu\right\rangle &= V_{\mu'}Z_\alpha X_{\mu\alpha}\left(V_{\mu'}^\dagger V_{\mu'}\right)\left|\psi_\nu^\mu\right\rangle = \exp(\mathrm{i}\xi_{\mu,\nu})V_{\mu'}\left|\psi_\nu^\mu\right\rangle \\ &= \exp(\mathrm{i}\varphi(\alpha, \mu'))Z_\alpha X_{(\mu+\mu')\alpha}V_{\mu'}\left|\psi_\nu^\mu\right\rangle, \end{aligned}$$

that is

$$Z_\alpha X_{(\mu+\mu')\alpha}\left[V_{\mu'}\left|\psi_\nu^\mu\right\rangle\right] = \exp(\mathrm{i}(\xi_{\mu,\nu} - \varphi(\alpha, \mu')))\left[V_{\mu'}\left|\psi_\nu^\mu\right\rangle\right], \tag{25}$$

i.e. the state $V_{\mu'}\left|\psi_{\nu}^{\mu}\right\rangle$ is an eigenstate of the set (23). This means that we can interpret the action of the V_μ operator as a 'rotation' in the discrete phase space,

$$\lambda_\mu \xrightarrow{V_{\mu'}} \lambda_{\mu+\mu'}, \tag{26}$$

although care should be taken in the case of fields $GF(2^n)$, as we will discuss below. Note that one cannot reach the vertical axis by applying V_μ to any other ray.

The explicit form of V_μ can be found taking into account that it is diagonal in the conjugate basis (24):

$$V_\mu = \sum_{\kappa\in GF(d)} c_{\kappa,\mu}|\widetilde{\kappa}\rangle\langle\widetilde{\kappa}|, \qquad c_{0,\mu} = 1. \tag{27}$$

Transforming the position operator Z_α with V_μ,

$$V_\mu Z_\alpha V_\mu^\dagger = \sum_{\kappa\in GF(d)} c_{\kappa+\alpha,\mu}c_{\kappa,\mu}^*|\widetilde{\kappa+\alpha}\rangle\langle\widetilde{\kappa}|$$

and taking into account that

$$Z_\alpha X_{\mu\alpha} = \sum_{\kappa\in GF(d)} \chi(-\mu\alpha\kappa)|\widetilde{\kappa+\alpha}\rangle\langle\widetilde{\kappa}|,$$

we find that the coefficients c_κ satisfy the following condition:

$$c_{\kappa+\alpha,\mu}c_{\kappa,\mu}^* = \exp(\mathrm{i}\varphi(\alpha,\mu))\chi(-\mu\alpha\kappa).$$

In particular, for $\kappa = 0$ we obtain

$$\exp(\mathrm{i}\varphi(\alpha,\mu)) = c_{\alpha,\mu}c_{0,\mu}^* = c_{\alpha,\mu}, \tag{28}$$

that is

$$c_{\kappa+\alpha,\mu}c_{\kappa,\mu}^* = c_{\alpha,\mu}\chi(-\mu\alpha\kappa), \tag{29}$$

and substituting $\alpha = 0$ we get $|c_{\kappa,\mu}|^2 = 1$, which also follows from the unitary condition $V_\mu V_\mu^\dagger = V_\mu^\dagger V_\mu = I$.

It is easy to note that equation (29) is automatically satisfied after the substitution

$$c_{\alpha,\mu} \to c_{\alpha,\mu}^{\nu} = c_{\alpha,\mu}\chi(-\alpha\nu),$$

which means that different sets of operators V_μ have the form

$$V_{\mu,\nu} = V_\mu X_\nu, \tag{30}$$

where V_μ is constructed using an arbitrary solution of equation (29).

3.3.1. Fields of odd characteristic. In the case of fields of odd characteristic, we impose an additional restriction on the rotation operators: we demand that V_μ form an Abelian group,

$$V_\mu V_{\mu'} = V_{\mu+\mu'}, \tag{31}$$

which implies that $c_{\kappa,\mu}c_{\kappa,\mu'} = c_{\kappa,\mu+\mu'}$ and in particular $c_{\kappa,\mu}^* = c_{\kappa,-\mu}$, leading to the relation $V_\mu^\dagger = V_{-\mu}$. In this case relation (26) is well defined, i.e. the operator V_μ transforms a state associated with the ray λ_μ into a state associated with the ray $\lambda_{\mu+\mu'}$. It can be shown (see below) that condition (31) cannot be satisfied for the fields of even characteristic, so that this case should be considered separately.

Then, a solution of equation (29) can be easily found,

$$c_{\kappa,\mu} = \chi(-2^{-1}\kappa^2\mu), \tag{32}$$

so that

$$V_\mu = \sum_{\kappa \in GF(d)} \chi(-2^{-1}\kappa^2\mu)|\widetilde{\kappa}\rangle\langle\widetilde{\kappa}|. \tag{33}$$

In the prime field case, $GF(p)$, $p \neq 2$, the whole set of rotation operators is produced by taking powers of a single operator [13]:

$$V = \sum_{k=0}^{p-1} \omega(-2^{-1}k^2)|\widetilde{k}\rangle\langle\widetilde{k}|.$$

In particular, the state $V^{m'}\left|\psi_0^m\right\rangle$ is associated with the ray $b = (m + m')a$, where the algebraic operations are mod p, so that

$$\lambda_0 \xrightarrow{V} \lambda_1, \qquad \underbrace{\lambda_0 \xrightarrow{V} \lambda_1 \xrightarrow{V} \lambda_2}_{V^2}, \quad \text{etc.}$$

3.3.2. Fields of even characteristic. The situation is more complicated for fields of char $(GF(d)) = 2$. In fact, it follows from (29) that (substituting $\kappa = \alpha$)

$$c_{\alpha,\mu}^2 = \chi(\alpha^2\mu). \tag{34}$$

The solution of the above equation is not unique and thus there is an ambiguity in solving equation (29) (see appendix B).

One of the consequences of this ambiguity is that operators of the form (27), where $c_{\kappa,\mu}$ is a *particular* (for a fixed value of μ and $\kappa \in GF(2^n)$) solution of (29), do not form a group. In particular, the operator V_μ^2 is not the identity operator. In fact, using (34) we have

$$V_\mu^2 = \sum_{\kappa \in GF(2^n)} c_{\kappa,\mu}^2|\widetilde{\kappa}\rangle\langle\widetilde{\kappa}| = \sum_{\kappa \in GF(2^n)} \chi(\kappa^2\mu)|\widetilde{\kappa}\rangle\langle\widetilde{\kappa}|,$$

which, due to the property $\operatorname{tr}\alpha = \operatorname{tr}\alpha^2$, $\alpha \in GF(2^n)$, can be transformed into

$$V_\mu^2 = \sum_{\kappa \in GF(2^n)} \chi\left(\kappa\mu^{2^{n-1}}\right)|\widetilde{\kappa}\rangle\langle\widetilde{\kappa}| = X_{\mu^{2^{n-1}}}, \tag{35}$$

where the relation $\kappa^2\mu = \left(\kappa\mu^{2^{n-1}}\right)^2$ has been used.

It also follows from (35) that inside the set $\{V_\mu, \mu \in GF(2^n)\}$ an inverse operator to a given V_μ from this set does not exist. To find the inverse operator to some V_μ we have to extend the set $\{V_\mu, \mu \in GF(2^n)\}$ to the whole collection of all the possible rotation operators defined in (30), i.e. to the set $\{V_{\mu,\nu}, \mu, \nu \in GF(2^n)\}$. Then, it is easy to conclude from (35) that

$$(V_{\mu,\nu})^{-1} = V_{\mu,\mu^{2^{n-1}}+\nu},$$

which implies the following relation between $c_{\alpha,\mu}$:

$$c_{\alpha,\mu}^* = \chi\left(\alpha\mu^{2^{n-1}}\right)c_{\alpha,\mu}. \tag{36}$$

We will fix the operator $V_{\mu,\nu=0}$ is such a way (see appendix B) that the coefficients $c_{\kappa,\mu}$, corresponding to the basis elements of the field, $\kappa = \sigma_1, \ldots, \sigma_n$, are chosen positive, so that we have

$$c_{\kappa,\mu} = \chi\left(\mu\sum_{i=1}^{n-1}k_i\sigma_i\sum_{j=i+1}^{n}k_j\sigma_j\right)\Pi_{l=1}^{n}\sqrt{\chi\left(k_l^2\sigma_l^2\mu\right)}, \tag{37}$$

$$\kappa = \sum_{i=1}^{n}k_i\sigma_i, \qquad k_i \in \mathcal{Z}_2, \tag{38}$$

where $\{\sigma_i, i = 1, \ldots, n\}$ are the elements of the basis and the principal branch of the square root in (37) is chosen. All the other possible rotating operators can be obtained according to (30).

The whole set of operators $\{V_{\mu,\nu}, \mu, \nu \in GF(2^n)\}$ form a group. Let us pick two operators V_μ and $V_{\mu'}$ constructed according to (37). Using the properties (24) and (28), we obtain

$$V_\mu V_{\mu'} Z_\alpha V_{\mu'}^\dagger V_\mu^\dagger = c_{\alpha,\mu}c_{\alpha,\mu'}Z_\alpha X_{(\mu+\mu')\alpha}. \tag{39}$$

On the other hand we have

$$V_{\mu+\mu'}Z_\alpha V_{\mu+\mu'}^\dagger = c_{\alpha,\mu+\mu'}Z_\alpha X_{(\mu+\mu')\alpha},$$

which suggests that (recall that $|c_{\alpha,\mu}| = 1$)

$$c_{\alpha,\mu}c_{\alpha,\mu'} = \exp(\mathrm{i}f(\alpha,\mu,\mu'))c_{\alpha,\mu+\mu'}, \tag{40}$$

where $f(\alpha,\mu,\mu') = f(\alpha,\mu',\mu)$ is a real function of α, μ, and μ'. Note that due to the property (29), the function $f(\alpha,\mu,\mu')$ depends linearly on the parameter α, in the sense that $f(\alpha+\beta,\mu,\mu') = f(\alpha,\mu,\mu') + f(\beta,\mu,\mu')$. The complex conjugate of (40) together with (36) leads to the condition $\exp(\mathrm{i}f(\alpha,\mu,\mu')) = \exp(-\mathrm{i}f(\alpha,\mu,\mu')) = \pm 1 \in \mathcal{Z}_2$. Because every linear map from $\alpha \in GF(p^n)$ to $GF(p) \simeq \mathcal{Z}_p$ is of the form of a character [7], $\alpha \to \chi(\alpha\beta)$, $\beta \in GF(p^n)$, the function $\exp(\mathrm{i}f(\alpha,\mu,\mu'))$ can be represented as

$$\exp(\mathrm{i}f(\alpha,\mu,\mu')) = \chi(\alpha f(\mu,\mu')).$$

It follows from (40) and from the above equation that there exists $\nu = f(\mu,\mu')$ (see appendix C) so that

$$V_\mu V_{\mu'} Z_\alpha V_{\mu'}^\dagger V_\mu^\dagger = X_\nu V_{\mu+\mu'} Z_\alpha V_{\mu+\mu'}^\dagger X_\nu^\dagger = c_{\alpha,\mu+\mu'}\chi(\alpha\nu)\, Z_\alpha X_{(\mu+\mu')\alpha}, \tag{41}$$

which immediately leads to the relation

$$V_\mu V_{\mu'} = V_{\mu+\mu'}X_{f(\mu,\mu')}.$$

Finally, in general we have

$$V_{\mu,\nu}V_{\mu',\nu'} = V_{\mu+\mu',\nu+\nu'+f(\mu,\mu')}.$$

3.4. Phase space construction

We can associate the lines in the discrete phase space with states in the Hilbert space according to the following construction.

1. The eigenstate of $\{Z_\alpha\}$ operators with all eigenvalues equal to 1, $|0\rangle = |\psi_0^0\rangle$, (note that such a state is unique) is associated with the horizontal axis $\beta = 0$. It is worth noting that such an association is arbitrary and in some sense fixes a definite class of quantum nets [2].

2. All the other states of the 'first' striation are obtained by applying the displacement operator X_ν to $|0\rangle$, so that the state $|\psi_\nu^0\rangle = X_\nu|0\rangle$ is associated with the horizontal line which crosses the vertical axis at the point $(0, \nu)$, i.e. with the line $\beta = \nu$. The states $|\psi_\nu^0\rangle$ are eigenstates of the set $\{Z_\alpha\}$,
$$Z_\alpha|\psi_\nu^0\rangle = \chi(\alpha\nu)X_\nu Z_\alpha|0\rangle = \chi(\alpha\nu)|\psi_\nu^0\rangle, \tag{42}$$
and form an orthonormal basis $\langle\psi_\nu^0|\psi_{\nu'}^0\rangle = \delta_{\nu\nu'}$.
3. All the other striations are constructed as follows: first we apply the rotation operator V_μ to the state $|0\rangle$ and the obtained state $|\psi_0^\mu\rangle = V_\mu|0\rangle$ is associated with the ray $\beta = \mu\alpha$. The state $|\psi_0^\mu\rangle$ is an eigenstate of the set $\{Z_\alpha X_{\mu\alpha}\}$ according to (25). It is worth noting that different sets of rotation operators can be chosen, which leads to different associations between states and lines (see discussion below).
4. All the other states of the μth striation are obtained by applying the operator X_ν to the state $|\psi_0^\mu\rangle$:
$$|\psi_\nu^\mu\rangle = X_\nu|\psi_0^\mu\rangle. \tag{43}$$
The states $|\psi_\nu^\mu\rangle$ are eigenstates of the set $\{Z_\alpha X_{\mu\alpha}\}$,
$$\begin{aligned}Z_\alpha X_{\mu\alpha}|\psi_\nu^\mu\rangle &= \exp(-\mathrm{i}\varphi(\alpha,\mu))V_\mu Z_\alpha V_\mu^\dagger X_\nu V_\mu|0\rangle\\ &= \exp(-\mathrm{i}\varphi(\alpha,\mu))V_\mu Z_\alpha X_\nu|0\rangle\\ &= \chi(\alpha\nu)\exp(-\mathrm{i}\varphi(\alpha,\mu))X_\nu V_\mu|0\rangle\\ &= \chi(\alpha\nu)\exp(-\mathrm{i}\varphi(\alpha,\mu))|\psi_\nu^\mu\rangle,\end{aligned}$$
and are associated with the lines $\beta = \mu\alpha + \nu$. The phase $\exp(-\mathrm{i}\varphi(\alpha,\mu))$ in the above equation is defined in (24).

Note that $|\psi_\nu^\mu\rangle = V_{\mu,\nu}|0\rangle$, where $V_{\mu,\nu}$ is defined in (30). As was shown in [12], the states (43) form mutually unbiased bases (MUBs) [17],
$$|\langle\psi_\nu^\mu|\psi_{\nu'}^{\mu'}\rangle|^2 = \frac{1}{d}, \qquad \mu \neq \mu',$$
which have been extensively discussed from different points of view in recent papers [11, 12, 18, 19]. In particular, it is known [2, 9] that different MUBs can be associated with different striations.

In our approach we note that the inner product of two states associated with lines can be rewritten as follows,
$$\begin{aligned}\langle\psi_\nu^\mu|\psi_{\nu'}^{\mu'}\rangle &= \langle 0|V_\mu^\dagger X_\nu^\dagger X_{\nu'}V_{\mu'}|0\rangle = \langle 0|X_{\nu'-\nu}V_{\mu'-\mu}|0\rangle\\ &= \sum_{\kappa\in GF(d)} c_{\kappa,\mu'-\mu}\langle\nu-\nu'|\widetilde{\kappa}\rangle\langle\widetilde{\kappa}|0\rangle,\end{aligned} \tag{44}$$
so that, taking into account $\langle\nu|\widetilde{\kappa}\rangle = \chi(\kappa\nu)/d^{1/2}$, we obtain
$$\langle\psi_\nu^\mu|\psi_{\nu'}^{\mu'}\rangle = \frac{1}{d}\sum_{\kappa\in GF(d)} c_{\kappa,\mu'-\mu}\chi(\kappa(\nu-\nu')) = \frac{1}{d}\Psi_{\nu,\nu'}^{\mu,\mu'}.$$
Then, we get
$$|\Psi_{\nu,\nu'}^{\mu,\mu'}|^2 = \sum_{\kappa,\kappa'\in GF(d)} c_{\kappa,\mu'-\mu}c_{\kappa',\mu'-\mu}^*\chi((\kappa-\kappa')(\nu-\nu')),$$

so that after changing the index $\kappa - \kappa' = \lambda$, and making use of relation (29) we immediately obtain

$$\left|\Psi^{\mu,\mu'}_{\nu,\nu'}\right|^2 = \sum_{\kappa',\lambda\in GF(d)} c_{\lambda,\mu'-\mu}\chi(-(\mu'-\mu)\lambda\kappa')\chi(\lambda(\nu-\nu'))$$
$$= \begin{cases} d^2\delta_{\nu,\nu'} & \mu = \mu' \\ \mathrm{d}\sum_{\lambda=0}^{p-1} c_{\lambda,\mu'-\mu}\chi(\lambda(\nu-\nu'))\delta_{0,\lambda} = d & \mu \neq \mu'. \end{cases}$$

The first relation corresponds to the inner product of states belonging to the same striation, i.e. to the same basis, and from the second relation one can observe that different striations correspond to different MUBs.

5. The state associated with the vertical axis β is obtained from $|0\rangle$ by applying the Fourier transform operator:

$$|\tilde{0}\rangle = F|0\rangle. \tag{45}$$

The state (45) is an eigenstate of the set $\{X_\beta, \beta \in GF(d)\}$ with all eigenvalues equal to unity: $X_\beta|\tilde{0}\rangle = |\tilde{0}\rangle$. The vertical lines, parallel to the axis β, crossing the axis α at the points $\alpha = \nu$ are associated with the states $\left|\tilde{\psi}^0_\nu\right\rangle = Z_\nu|\tilde{0}\rangle$, which are eigenstates of the set $\{X_\beta\}$:

$$X_\beta\left|\tilde{\psi}^0_\nu\right\rangle = \chi(-\beta\nu)Z_\nu X_\beta|\tilde{0}\rangle = \chi(-\beta\nu)\left|\tilde{\psi}^0_\nu\right\rangle.$$

It is clear that

$$\left|\langle\psi^\mu_\nu|\tilde{\psi}^0_{\nu'}\rangle\right|^2 = \frac{1}{d}.$$

For the fields of odd characteristics we can always choose the set of rotation operators in such a way that they form a group, which in particular means that a consecutive application of any V_μ from this set returns us to the initial state: $V^p_\mu = I$. This does not hold for the fields of even characteristic due to equation (35), which can be interpreted as follows: the first application of the rotation operator V_μ transforms a state associated with the ray of some striation to a state corresponding to a ray from another striation. The second application of V_μ does not return to the initial state (as could be expected from (26)), but to a state which belongs to the original striation but displaced by $X_{\mu^{2^{n-1}}}$. So that, from the geometrical point of view the operator V^2_μ for $GF(2^n)$ transforms a ray from some striation to a parallel line from the same striation.

3.5. The phase of the displacement operator

The phase $\varphi(\alpha, \mu)$ which appears in (24) is intimately related to the phase $\phi(\alpha, \beta)$ of the displacement operator (9). Let us impose the natural condition that the sum of the Wigner function along the line $\beta = \mu\alpha + \nu$ is equal to the average value of the density matrix over the state $\left|\psi^\mu_\nu\right\rangle$ associated with that line [1]:

$$\frac{1}{d}\sum_{\alpha,\beta\in GF(d)} W(\alpha,\beta)\delta_{\beta,\mu\alpha+\nu} = \left\langle\psi^\mu_\nu\right|\rho\left|\psi^\mu_\nu\right\rangle, \tag{46}$$

where

$$W(\alpha,\beta) = \mathrm{Tr}[\rho\Delta(\alpha,\beta)]. \tag{47}$$

According to the general construction, the state $\left|\psi_\nu^\mu\right\rangle$ is obtained by application of the operator $V_{\mu,\nu}$ to the state $|0\rangle$: $\left|\psi_\nu^\mu\right\rangle = V_{\mu,\nu}|0\rangle$. After simple algebra we transform the left-hand side of (46) as follows:

$$\frac{1}{d}\sum_{\alpha,\beta\in GF(d)} W(\alpha,\beta)\delta_{\beta,\mu\alpha+\nu} = \frac{1}{d}\sum_{\alpha\in GF(d)} W(\alpha,\mu\alpha+\nu)$$

$$= \frac{1}{d}\sum_{\kappa,\lambda\in GF(d)} \rho_{\kappa,\lambda}\phi(\mu^{-1}(-\kappa+\lambda),-\kappa+\lambda)\chi(\mu^{-1}(\kappa+\lambda)(\lambda+\nu)), \tag{48}$$

where $\rho = \sum_{\kappa,\lambda}\rho_{\kappa,\lambda}|\kappa\rangle\langle\lambda|$; meanwhile the right-hand part is converted into

$$\left\langle\psi_\nu^\mu\right|\rho\left|\psi_\nu^\mu\right\rangle = \langle 0|V_\mu^\dagger X_\nu^\dagger \rho X_\nu V_\mu|0\rangle$$

$$= \frac{1}{d^2}\sum_{\kappa,\kappa',\tau,\upsilon\in GF(d)} \rho_{\tau,\upsilon}c^*_{\kappa,\mu}c_{\kappa',\mu}\chi(-\kappa(\tau-\nu)+\kappa'(\upsilon-\nu)).$$

Taking into account relation (29), the above equation can be rewritten as follows:

$$\left\langle\psi_\nu^\mu\right|\rho\left|\psi_\nu^\mu\right\rangle = \frac{1}{d}\sum_{\kappa,\lambda}\rho_{\kappa,\lambda}c_{\mu^{-1}(-\kappa+\lambda),\mu}\chi(\mu^{-1}(\kappa+\lambda)(\lambda+\nu)). \tag{49}$$

Comparing (48) and (49) we observe that $\phi(\mu^{-1}(-\kappa+\lambda),-\kappa+\lambda) = c_{\mu^{-1}(-\kappa+\lambda),\mu}$, or in a compact form

$$\phi(\tau,\upsilon) = c_{\tau,\tau^{-1}\upsilon}. \tag{50}$$

Also, we impose the conditions $\phi(\tau,0) = \phi(0,\upsilon) = 1$, which mean that the displacements along the axes α and β, which are performed by applying Z_κ and X_λ operators correspondingly, do not generate any phase.

This immediately implies that for fields of odd characteristic

$$\phi(\tau,\upsilon) = \chi(-2^{-1}\tau\upsilon), \tag{51}$$

and condition (11) is automatically satisfied. Thus, the displacement operator in this case has the form

$$D(\alpha,\beta) = \chi(-2^{-1}\alpha\beta)Z_\alpha X_\beta \tag{52}$$

so that the unitary condition $D^\dagger(\alpha,\beta) = D(-\alpha,-\beta)$ is satisfied and the kernel (13) can be represented in the familiar form

$$\Delta(\alpha,\beta) = D(\alpha,\beta)PD^\dagger(\alpha,\beta),$$

where

$$P = \frac{1}{d}\sum_{\alpha,\beta\in GF(d)} D(\alpha,\beta), \qquad P|\alpha\rangle = |-\alpha\rangle,$$

is the *parity operator*.

In general, for a density matrix defined in the standard basis $|\alpha\rangle$ as

$$\rho = \sum_{\mu,\nu\in GF(d)} \rho_{\mu,\nu}|\mu\rangle\langle\nu|, \tag{53}$$

the Wigner function takes the form

$$W_\rho(\alpha,\beta) = \frac{1}{d}\sum_{\gamma,\mu,\nu\in GF(d)} \chi(\gamma(\nu-\beta)+\alpha(\nu-\mu))\phi(\gamma,\nu-\mu)\rho_{\mu,\nu}, \tag{54}$$

which still can be simplified (summed over γ) for the fields of odd characteristics taking into account the explicit expression (51) for the phase ϕ.

Nevertheless, for the fields of even characteristic, $d = 2^n$, there is a freedom in the election of the phase ϕ, which takes values $\pm 1, \pm \mathrm{i}$, related to different possibilities of choosing the rotation operators $V_{\mu,\nu} = V_\mu X_\nu$ for the phase space construction. Once the set $\{V_{\mu,\nu}\}$ of rotation operators is fixed we can find the phase ϕ from (50) and thus construct the Wigner function (54).

Using relation (47) we can find the Wigner function for the state (43) corresponding to the line $\beta = \mu\alpha + \nu$. First of all, using (27) and the property $\langle\tilde{\kappa}|\lambda\rangle = \chi(-\kappa\lambda)/d^{1/2}$, we rewrite the state $\left|\psi_\nu^\mu\right\rangle$ as follows:

$$\left|\psi_\nu^\mu\right\rangle = \frac{1}{\sqrt{d}} \sum_{\kappa\in GF(d)} c_{\kappa,\mu}\chi(-\kappa\nu)|\tilde{\kappa}\rangle = \frac{1}{d} \sum_{\kappa,\lambda\in GF(d)} c_{\kappa,\mu}\chi(\kappa(\lambda-\nu))|\lambda\rangle.$$

Then, from (13) and (47) we obtain after long but straightforward algebra,

$$W_{|\psi_\nu^\mu\rangle}(\alpha,\beta) = \left\langle\psi_\nu^\mu\right|\Delta(\alpha,\beta)\left|\psi_\nu^\mu\right\rangle = \delta_{\beta,\mu\alpha+\nu},$$

for fields of both odd and even characteristic independently of the choice of the rotation operator in the last case.

3.6. Non-uniqueness of the Wigner function

It is worth noting that the Wigner function constructed using different distributions of signs in V_μ operators are not trivially related to each other. This difference is of fundamental significance for fields of even characteristic (because there is no natural choice of the set of rotation operators), although similar considerations can also be taken into account for fields of odd characteristic (if a different set of rotation operators to (33) is used for the phase-space construction).

In the rest of this section we will focus on fields of even characteristic. Let us fix the operators V_μ according to (37) and choose some other set, so that $V_{\mu,h(\mu)} = V_\mu X_{h(\mu)}$, where $h(\mu)$ is an arbitrary function satisfying the following conditions: (a) $h(0) = 0$, which basically means that even after changing the rotation operators, the displacement operators along the axes α and β have no phases, $D(\alpha,0) = Z_\alpha, D(0,\beta) = X_\beta$; (b) the non-singularity: $\alpha h(\alpha^{-1}\beta) = 0$, if $\alpha = 0$ for any $\beta \in GF(2^n)$, which implies that the coefficient $c_{0,\mu}$ in (27) is fixed, $c_{0,\mu} = 1$, for all V_μ. The simplest example of such a function can be given in the case where rotation operators are labelled with powers of a primitive element σ: $\{V_\mu, \mu \in GF(2^n)\} = \{V_{\sigma^k}, k = 1,\ldots,2^n-1\}$, then $h(\sigma^k) = \sigma^{m(k)}$, where m is a natural number which depends on the value of k.

The Wigner function constructed using the new rotation operators $V_{\mu,\nu}$ has the form

$$W'_\rho(\alpha,\beta) = \mathrm{Tr}[\rho\Delta'(\alpha,\beta)], \qquad \Delta'(\alpha,\beta) = \frac{1}{2^n}\sum_{\kappa,\lambda\in GF(2^n)} \chi(\alpha\lambda-\beta\kappa)D'(\kappa,\lambda),$$

where

$$D'(\kappa,\lambda) = c'_{\kappa,\kappa^{-1}\lambda}Z_\kappa X_\lambda,$$

and $c'_{\kappa,\xi}$ are the matrix elements (27) of $V_{\mu,h(\mu)}$ in the conjugate basis $|\tilde{\alpha}\rangle$, so that

$$c'_{\kappa,\kappa^{-1}\lambda} = \chi(\kappa h(\kappa^{-1}\lambda))c_{\kappa,\kappa^{-1}\lambda}.$$

Then, we have

$$\begin{aligned} D'(\kappa,\lambda) &= \chi(\kappa h(\kappa^{-1}\lambda))c_{\kappa,\kappa^{-1}\lambda}Z_\kappa X_\lambda \\ &= c_{\kappa,\kappa^{-1}\lambda}X_{h(\kappa^{-1}\lambda)}Z_\kappa X_{h(\kappa^{-1}\lambda)}X_\lambda \\ &= X_{h(\kappa^{-1}\lambda)}D(\kappa,\lambda)X_{h(\kappa^{-1}\lambda)}. \end{aligned}$$

After some simple algebra we obtain the 'new' Wigner function $W'_\rho(\alpha,\beta)$ in terms of the coefficients of expansion (53),

$$W'_\rho(\alpha,\beta) = \frac{1}{2^n}\sum_{\mu,\nu,\gamma\in GF(2^n)} \rho_{\mu,\nu} \tag{55}$$

$$\chi(\alpha(\nu-\mu)-\beta\gamma+\gamma h(\gamma^{-1}(\nu-\mu))+\gamma\nu)\phi(\gamma,\nu-\mu), \tag{56}$$

which is related to the 'old' Wigner function (constructed with V_μ operators) as follows:

$$W'_\rho(\alpha,\beta) = \frac{1}{2^n}\sum_{\substack{\gamma'\in GF(2^n)\\ \gamma\neq 0}} W_\rho(\alpha+\gamma h(\gamma^{-1})+\gamma\gamma',\beta+\gamma') \tag{57}$$

$$+\frac{1}{2^n}\sum_{\beta\in GF(2^n)} W_\rho(\alpha,\beta)+\frac{1}{2^n}\sum_{\alpha\in GF(2^n)} W_\rho(\alpha,\beta)-1. \tag{58}$$

Note that

$$p(\alpha)=\sum_{\beta\in GF(2^n)} W_\rho(\alpha,\beta), \qquad \widetilde{p}(\beta)=\sum_{\alpha\in GF(2^n)} W_\rho(\alpha,\beta)$$

are the marginal probabilities to detect the system at the states $|\alpha\rangle$ and $|\tilde{\beta}\rangle$, respectively.

It is clear that the sum of the 'new' Wigner function over a line $\beta=\mu\alpha+\nu$ gives the same result as the sum of the 'old' Wigner function over the points of the shifted line $\beta=\mu\alpha+\nu+h(\mu)$:

$$\sum_{\alpha,\beta\in GF(2^n)} W'(\alpha,\beta)\delta_{\beta=\mu\alpha+\nu} = \sum_{\alpha,\beta\in GF(2^n)} W(\alpha,\beta)\delta_{\beta=\mu\alpha+\nu+h(\mu)}.$$

For a particular choice $h(\mu)=\kappa$ - $const$, $h(0)=0$, we find that the new Wigner function has the form

$$W'_\rho(\alpha,\beta)=W_\rho(\alpha,\beta+\kappa)-\rho_{\beta+\kappa,\beta+\kappa}+\rho_{\beta,\beta}. \tag{59}$$

For a more complicated case $h(\xi)=\kappa\xi$, the Wigner function acquires the following form:

$$W'_\rho(\alpha,\beta)=W_\rho(\alpha+\kappa,\beta)+\frac{1}{2^n}p(\alpha)-\frac{1}{2^n}p(\alpha+\kappa).$$

As we have seen above, the Wigner function of any state of the form (53) with $\rho_{\mu,\nu}=q_\mu\delta_{\mu,\nu}$ does not depend on the choice of sign (and thus is uniquely defined), as can be observed directly from (55) in the case of $GF(2^n)$.

As a non-trivial example of essentially different Wigner functions which can be associated with the same state let us consider a particular case of real symmetric density matrices $\rho_{\mu,\nu}=\rho_{\nu,\mu}$. For this class of states the Wigner function (55) can be rewritten in the following explicitly symmetric form:

$$W'_\rho(\alpha,\beta)=\frac{1}{2^{n+1}}\sum_{\substack{\mu\neq\nu\in GF(2^n)\\ \gamma\neq 0}} \rho_{\mu,\nu}\chi(\alpha(\nu+\mu)+\beta\gamma+\gamma h(\gamma^{-1}(\nu+\mu)))$$

$$\times\phi(\gamma,\nu+\mu)[\chi(\gamma\nu)+\chi(\gamma\mu)]+\frac{1}{2^n}\sum_{\mu\neq\nu\in GF(2^n)} \rho_{\mu,\nu}\chi(\alpha(\nu-\mu))+\rho_{\beta,\beta}.$$

Now, we observe from the above equation that if the factor $[\chi(\gamma\nu)+\chi(\gamma\mu)]$ is zero, the Wigner function obviously does not depend on the choice of the function $h(\nu)$. Thus, two

Wigner functions corresponding to functions $h_1(\nu)$ and $h_2(\nu)$ are the same if simultaneously $\chi(\gamma h_1(\gamma^{-1}(\nu+\mu))) = \chi(\gamma h_2(\gamma^{-1}(\nu+\mu)))$ and $\chi(\gamma\nu)+\chi(\gamma\mu) \neq 0$ or, in other words,

$$\mathrm{tr}(\gamma[h_1(\gamma^{-1}(\nu+\mu)) + h_2(\gamma^{-1}(\nu+\mu))]) = 0, \tag{60}$$

$$\mathrm{tr}(\gamma[\mu+\nu]) = 0, \tag{61}$$

where $\gamma \neq 0$ and $\mu \neq \nu$.

For instance, consider the state $|\psi\rangle = (|0\rangle + |\sigma^3\rangle)/\sqrt{2}$ in the case $GF(2^2)$ and fix the irreducible polynomial as $\sigma^2+\sigma+1=0$. The indices μ and ν in (60)–(61) take values 0 and σ^3, so that $\mu+\nu=\sigma^3$, and thus it follows from (61) that the only admissible value of γ is $\gamma=\sigma^3$. Then, condition (60) leads to the following equation for the functions $h_1(\nu)$ and $h_2(\nu)$:

$$h_1(\sigma^3) + h_2(\sigma^3) = \sigma^3. \tag{62}$$

The first set of solutions is $h_1(\sigma^3) = \sigma, h_2(\sigma^3) = \sigma^2$ and correspondingly $h_1(\sigma^3) = \sigma^2, h_2(\sigma^3) = \sigma$. This means that two sets of rotation operators

$$1. \quad X_\kappa V_\sigma,\ X_\lambda V_{\sigma^2},\ X_\sigma V_{\sigma^3}, \tag{63}$$

$$2. \quad X_{\kappa'} V_\sigma,\ X_{\lambda'} V_{\sigma^2},\ X_{\sigma^2} V_{\sigma^3}, \tag{64}$$

where $\kappa, \kappa', \lambda, \lambda' \in GF(2^2)$ lead to the same Wigner function. Note that the constants $\kappa, \kappa', \lambda, \lambda'$ are arbitrary elements of $GF(2^2)$ because there are no restrictions imposed either on $h(\sigma)$ or $h(\sigma^2)$.

The second set of solutions of (62) is $h_1(\sigma^3) = \sigma^3, h_2(\sigma^3) = 0$ and, correspondingly, $h_1(\sigma^3) = 0, h_2(\sigma^3) = \sigma^3$, so that the rotation operators,

$$3. \quad X_{\kappa''} V_\sigma,\ X_{\lambda''} V_{\sigma^2},\ X_{\sigma^3} V_{\sigma^3}, \tag{65}$$

$$4. \quad X_{\kappa'''} V_\sigma,\ X_{\lambda'''} V_{\sigma^2},\ V_{\sigma^3}, \tag{66}$$

with $\kappa'', \kappa''', \lambda'', \lambda''' \in GF(2^2)$ produce the same Wigner functions.

Finally, there are only two different Wigner functions to represent the state $|\psi\rangle = (|0\rangle + |\sigma^3\rangle)/\sqrt{2}$ (compare with [5]). It is worth noting that this state is labelled by the elements of the field $GF(2^2)$ and thus has no direct relation to the physical state, until the basis for the field representation is fixed (see section 6).

In figure 1(*a*) we plot the Wigner function for the state $|\psi\rangle = (|0\rangle + |\sigma^3\rangle)/\sqrt{2}$ using the following choice of the rotation operators

$$V_\sigma = \mathrm{Diag}(1,1,i,-i), \qquad V_{\sigma^2} = \mathrm{Diag}(1,i,-1,i), \qquad V_{\sigma^3} = \mathrm{Diag}(1,i,-i,1),$$

which corresponds to the case (64) with $X_{\kappa'} = I$, $X_{\lambda'} = X_{\sigma^2}$.

In figure 1(*b*) we plot the Wigner function for the same state *but* using another choice of the rotation operators

$$V_\sigma = \mathrm{Diag}(1,1,i,-i), \qquad V_{\sigma^2} = \mathrm{Diag}(1,i,1,-i), \qquad V_{\sigma^3} = \mathrm{Diag}(1,i,i,-1),$$

corresponding to the case (66) with $X_{\kappa'''} = X_{\lambda'''} = I$.

Obviously, for larger fields the variety of Wigner functions for a given state rapidly grows with the dimension of the field even for highly symmetrical states. For instance, the state $|\psi\rangle = (|0\rangle + |\sigma^7\rangle)/\sqrt{2}$ labelled with elements of $GF(2^3)$ can be represented in eight different ways. In figures 2(*a*)–(*h*) we plot Wigner functions for different non-trivial choices of the set of rotation operators, where the initial 'bare' set of rotation operators is fixed as follows,

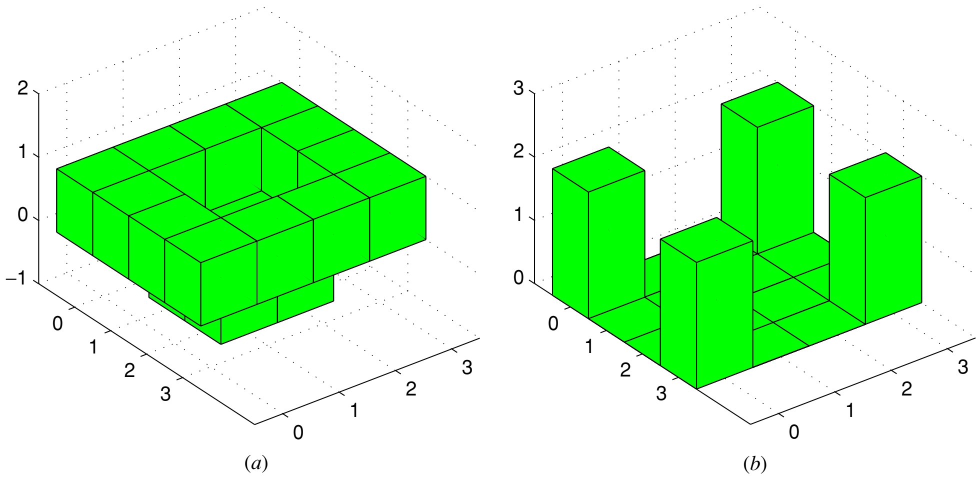

Figure 1. (*a*)–(*b*) Wigner function for the state $|\psi\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |\sigma^3\rangle]$ defined on $GF(2^2)$. The set of rotation operators: (*a*) $V_\sigma = \mathrm{Diag}(1, 1, i, -i)$, $V_{\sigma^2} = \mathrm{Diag}(1, i, -1, i)$, $V_{\sigma^3} = \mathrm{Diag}(1, i, -i, 1)$; (*b*) $V_\sigma = \mathrm{Diag}(1, 1, i, -i)$, $V_{\sigma^2} = \mathrm{Diag}(1, i, 1, -i)$, $V_{\sigma^3} = \mathrm{Diag}(1, i, i, -1)$.

$$V_\theta = \mathrm{Diag}(1, 1, 1, i, i, -i, -1, i), \qquad V_{\sigma^2} = \mathrm{Diag}(1, i, 1, -i, 1, -1, i, i), \tag{67}$$

$$V_{\sigma^3} = \mathrm{Diag}(1, 1, i, i, -i, -1, i, 1), \qquad V_{\sigma^4} = \mathrm{Diag}(1, 1, i, -1, 1, i, -i, i), \tag{68}$$

$$V_{\sigma^5} = \mathrm{Diag}(1, i, i, -i, -1, i, 1, 1), \qquad V_{\sigma^6} = \mathrm{Diag}(1, i, 1, -1, -i, -i, -i, 1) \tag{69}$$

$$V_{\sigma^7} = \mathrm{Diag}(1, i, i, 1, -i, 1, -1, i), \tag{70}$$

and the minimal polynomial is chosen as $\sigma^3 + \sigma^2 + 1 = 0$.

For fields of odd characteristic, in the whole group $\{V_\mu X_\nu, \mu, \nu \in GF(p^n)\}$ a subgroup containing only rotation operators $\{V_\mu, \mu \in GF(p^n)\}$ can be separated, which allows us to construct the phase space as outlined in previous sections, so that the Wigner function is uniquely defined for a given state. Nevertheless, the whole group can be used for phase-space construction as well, which would lead to non-uniqueness in the definition of the Wigner function, very similar to (57).

For an arbitrary state, we can easily calculate a total number of possible Wigner functions which represent this state in the discrete phase space. According to the present construction, we fix the phase of the state corresponding to the horizontal line (42). Also, we fix the property (7) of the Fourier transform operator (6), i.e. the Fourier transformation of Z_α operators generate X_α operators without any phase factor (which in principle is not necessary if the property $F^4 = I$ for $d = p^n$, where $p \neq 2$ and $F^2 = I$ for $d = 2^n$ is not required). Now, we can generate all the possible Wigner functions choosing $(d-1)$ different rotation operators $V_\mu X_\nu$ (both for fields of odd and even characteristics), which gives d^{d-1} different structures (which is directly related to different quantum nets introduced in [2]). Nevertheless, the symmetry of the state can essentially reduce the number of different Wigner functions.

4. Reconstruction procedure

It is well known that the Wigner function can be reconstructed using projective measurements, associated with a summation over the lines [1, 20]. In this section we explicitly relate the

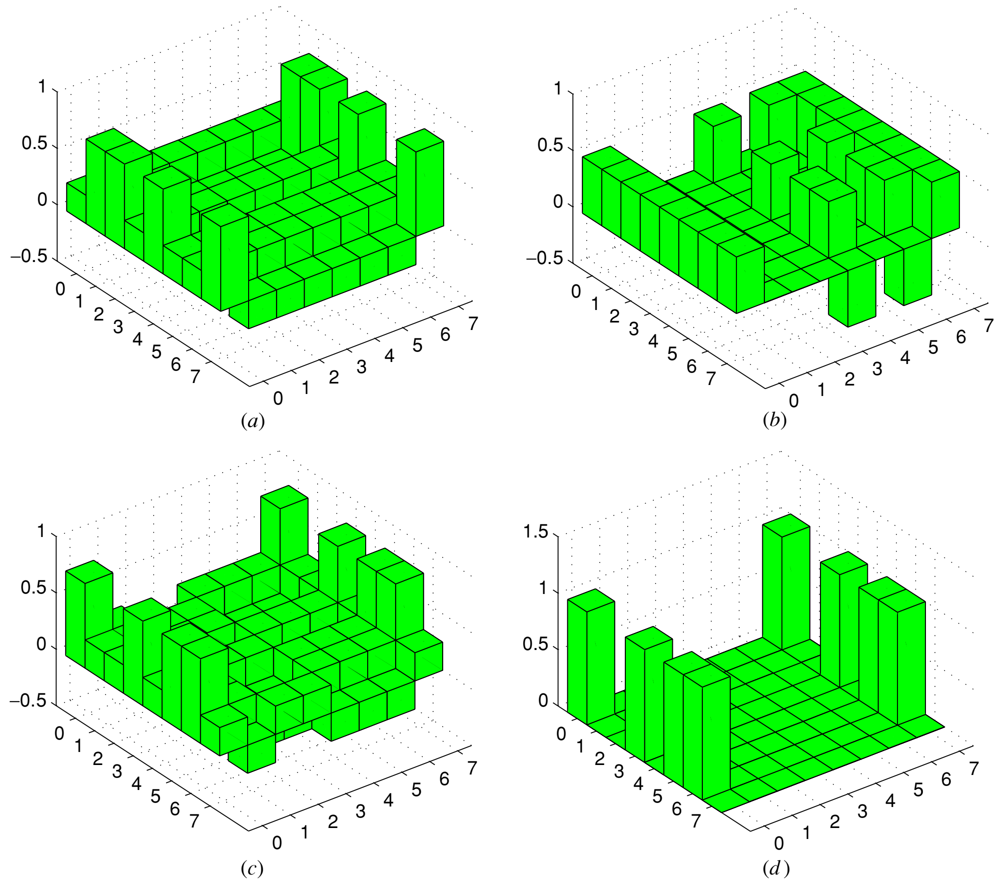

Figure 2. (*a*)–(*h*) Wigner function for the state $|\psi\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |\sigma^7\rangle]$ defined on $GF(2^3)$. The set of rotation operators: (*a*) $V_\sigma, V_{\sigma^2}, V_{\sigma^3}, V_{\sigma^4}, V_{\sigma^5}, V_{\sigma^6}, V_{\sigma^7}$, where V_{σ^n} are defined in (67)–(70); (*b*) $X_\sigma V_\sigma, V_{\sigma^2}, V_{\sigma^3}, V_{\sigma^4}, V_{\sigma^5}, V_{\sigma^6}, V_{\sigma^7}$; (*c*) $X_\sigma V_\sigma, X_{\sigma^2} V_{\sigma^2}, V_{\sigma^3}, V_{\sigma^4}, V_{\sigma^5}, V_{\sigma^6}, V_{\sigma^7}$; (*d*) $X_\sigma V_\sigma, X_{\sigma^2} V_{\sigma^2}, V_{\sigma^3}, X_{\sigma^4} V_{\sigma^4}, V_{\sigma^5}, V_{\sigma^6}, V_{\sigma^7}$; (*e*) $X_{\sigma^4} V_\sigma, X_{\sigma^2} V_{\sigma^2}, V_{\sigma^3}, X_{\sigma^4} V_{\sigma^4}, V_{\sigma^5}, V_{\sigma^6}, V_{\sigma^7}$; (*f*) $X_{\sigma^4} V_\sigma, X_\sigma V_{\sigma^2}, V_{\sigma^3}, X_{\sigma^4} V_{\sigma^4}, V_{\sigma^5}, V_{\sigma^6}, V_{\sigma^7}$; (*g*) $X_{\sigma^7} V_\sigma, X_\sigma V_{\sigma^2}, V_{\sigma^3}, X_{\sigma^7} V_{\sigma^4}, V_{\sigma^5}, V_{\sigma^6}, V_{\sigma^7}$; (*h*) $X_{\sigma^3} V_\sigma, X_{\sigma^7} V_{\sigma^2}, V_{\sigma^3}, X_{\sigma^5} V_{\sigma^4}, V_{\sigma^5}, V_{\sigma^6}, V_{\sigma^7}$.

elements of the density matrix with the corresponding tomogram, the averages of the form $\langle \psi_\nu^\mu | \rho | \psi_\nu^\mu \rangle = \omega(\mu, \nu)$.

Let us start with the relation of the tomogram $\omega(\mu, \nu)$ with the Wigner function,

$$\omega(\mu, \nu) = \frac{1}{d} \sum_{\alpha, \beta \in GF(d)} W(\alpha, \beta) \delta_{\beta, \mu\alpha + \nu} = \frac{1}{d} \sum_{\alpha \in GF(d)} W(\alpha, \mu\alpha + \nu), \tag{71}$$

and consequently with the components of the density matrix in the basis of the displacement operators (16), which is obtained by taking into account relation (17):

$$\omega(\mu, \nu) = \sum_{\kappa \in GF(d)} \rho_{\kappa, \mu\kappa} \chi(\kappa\nu).$$

The above equation can immediately be inverted using (4),

$$\rho_{\kappa, \mu\kappa} = \frac{1}{d} \sum_{\nu \in GF(d)} \omega(\mu, \nu) \chi(-\kappa\nu),$$

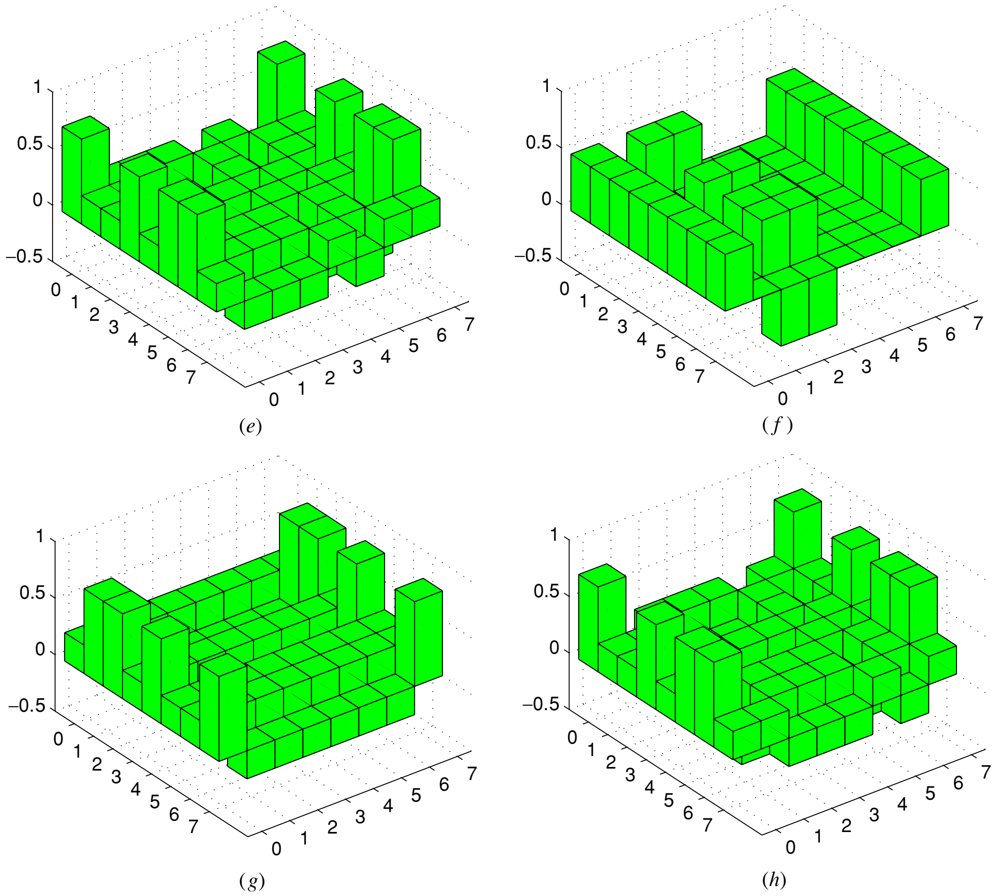

Figure 2. (Continued.)

or, changing the indices

$$\rho_{\kappa,\lambda} = \frac{1}{d} \sum_{\nu \in GF(d)} \omega(\kappa^{-1}\lambda, \nu)\chi(-\kappa\nu),$$

where $\kappa \neq 0$.

To reconstruct the matrix element $\rho_{0,\lambda}$ we have to use the results of measurements in the conjugate basis $|\widetilde{\kappa}\rangle$,

$$\omega(\kappa) = \langle\widetilde{\kappa}|\rho|\widetilde{\kappa}\rangle = \frac{1}{d} \sum_{\alpha,\beta \in GF(d)} W(\alpha, \beta)\delta_{\alpha,\kappa} = \sum_{\lambda \in GF(d)} \rho_{0,\lambda}\chi(-\kappa\lambda),$$

which leads to

$$\rho_{0,\lambda} = \frac{1}{d} \sum_{\kappa \in GF(d)} \omega(\kappa)\chi(\kappa\lambda).$$

5. Ordering the points on the axes

In order to plot the Wigner function we have to choose an arrangement of the field elements and take it into account to fix the order of the elements on the axes in the finite plane $GF(d) \times GF(d)$. When the dimension of the system is a prime number there is a natural ordering of the elements, i.e. for any $a, b \in \mathcal{Z}_p, a \neq b$ there is a relation either $a < b$ or $a > b$, so that the points on the axes can be enumerated. For instance, in the case of $\mathcal{Z}_5$ the elements are arranged as $\{0, 1, 2, 3, 4\}$.

For field extensions there is no natural ordering of elements; however, there are several possibilities of arranging the elements of the field. The most common choice is an ordering according to powers (which are natural numbers and thus can be naturally ordered) of some primitive element. Nevertheless, the primitive element, in general, is not unique. Actually, for the d-dimensional system there are $\phi(d-1)$ primitive elements, where $\phi(r)$ is Euler's function, which indicates the number of integers with $1 \leqslant n \leqslant r$ which are relatively prime to r [7].

As another possibility we can enumerate the points on the axes according to the following procedure: firstly, we fix that the origin corresponds to the point $(0, 0)$; secondly, we choose some basis $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ in the field $GF(p^n)$ and expand elements in this basis: $\alpha = \sum_{j=1}^{n} a_j \sigma_j, a_j \in \mathcal{Z}_p$. Now, we arrange the expansion coefficients in a sequence to form a number on the base p (binary, ternary system, etc) starting with the coefficient a_n taking the leftmost place; it will be followed by a_{n-1} and so on; obviously, a_1 takes the rightmost place. The full number is $(a_n a_{n-1} \ldots a_1)_p$ and it can be transformed into some integer in the decimal basis using the standard procedure: $(a_1 \times p^0) + (a_2 \times p^1) + \cdots + (a_n \times p^{n-1})$. This procedure is obviously not unique due to the existence of different bases in the field. As an example, let us take $GF(2^3)$, the choice of the irreducible polynomial as $x^3 + x^2 + 1 = 0$, and use the normal self-dual basis $\{\sigma, \sigma^2, \sigma^4\}$; in this basis the field elements are

$$\begin{array}{ll} \theta = \theta, & \theta^2 = \theta^2, \\ \theta^3 = \theta + \theta^4, & \theta^4 = \theta^4, \\ \theta^5 = \theta^2 + \theta^4, & \theta^6 = \theta + \theta^2, \\ \theta^7 = \theta + \theta^2 + \theta^4, & 0. \end{array}$$

Now, we can associate each element with a number in the binary system:

$$\begin{array}{ll} \theta \to (100)_2 \to (4)_{10}, & \theta^2 \to (010)_2 \to (2)_{10}, \\ \theta^3 \to (101)_2 \to (5)_{10}, & \theta^4 \to (001)_2 \to (1)_{10}, \\ \theta^5 \to (011)_2 \to (3)_{10}, & \theta^6 \to (110)_2 \to (6)_{10}, \\ \theta^7 \to (111)_2 \to (7)_{10}, & 0 \to (000)_2 \to (0)_{10}. \end{array}$$

So, we arrange the points on the axes using the above ordering according to $\{0, \theta^4, \theta^2, \theta^5, \theta, \theta^3, \theta^6, \theta^7\}$.

Another possibility for arranging the elements of the field is in accordance with the value of the trace of each element (which is a natural number) [10] and inside the set of the elements with the same trace we can use any of the above-mentioned ordering, say powers of a primitive element.

6. From abstract states to physical states

In applications we have to establish a relation between abstract states labelled with elements of the field and states of a given physical system. Such interrelation strongly depends on the character of a system, for instance, if the system is actually a single 'particle' with p^n energy levels or it consists of n 'particles' (degrees of freedom) with p energy levels. In the last case the mapping $\mathcal{H}_d \Leftrightarrow \mathcal{H}_p \otimes \mathcal{H}_p \ldots \otimes \mathcal{H}_p$ from the abstract Hilbert space to n-particle vector space can be achieved by expanding an element of the field in a convenient basis $\{\sigma_1, \ldots, \sigma_n\}$: $\alpha = a_1\sigma_1 + \cdots + a_n\sigma_n$, $a_j \in \mathcal{Z}_p$, so that

$$|\alpha\rangle \rightarrow |a_1\rangle_1 \otimes \cdots \otimes |a_n\rangle_n \equiv |a_1, \ldots, a_n\rangle,$$

and the coefficients a_j play the role of quantum numbers of each particle. For instance, in the case $GF(2^2)$ the state $(|0\rangle + |\sigma^3\rangle)/\sqrt{2}$ corresponds to the physical state $(|00\rangle + |10\rangle)/\sqrt{2}$ in the polynomial basis $(1, \sigma)$, whereas in the self-dual basis (σ, σ^2) it is associated with $(|00\rangle + |11\rangle)/\sqrt{2}$. Observe that while one state is factorizable, the other one is entangled. Also, it is worth noting that in the case of $GF(2^3)$ the state $(|0\rangle + |\sigma^7\rangle)/\sqrt{2}$, studied in section 3.6, corresponds to the physical state $(|000\rangle + |111\rangle)/\sqrt{2}$ in the self-dual basis, which, for the primitive polynomial $x^3 + x^2 + 1 = 0$, has the form $(\sigma, \sigma^2, \sigma^4)$.

This implies that all the operators Z_β are factorized into a product of single particle Z operators (5), $Z_\beta = Z^{b_1} \otimes \cdots \otimes Z^{b_n}$, where $\beta = b_1'\sigma_1' + \cdots + b_n'\sigma_n'$ and $\{\sigma_1', \ldots, \sigma_n'\}$ is the basis which is dual to $\{\sigma_1, \ldots, \sigma_n\}$ (see appendix A) and $b_i' \in \mathcal{Z}_p$. To have a better understanding of this aspect let us recall the definition of the operator Z_α,

$$Z_\alpha = \sum_{\beta \in GF(d)} \chi(\alpha\beta)|\beta\rangle\langle\beta|,$$

and choose a basis $\{\sigma_1, \ldots, \sigma_n\}$ to expand β. Then, taking $\alpha = \sigma_i'$ as an element of the dual basis, we obtain

$$Z_{\sigma_i'} = \sum_{\beta \in GF(d)} \chi(\sigma_i'\beta)|\beta\rangle\langle\beta| = \Pi_{j=1}^n \sum_{b_j=0}^{p-1} \exp\left(\frac{2\pi \mathrm{i}}{p}\,\mathrm{tr}(\sigma_i'\sigma_j)\right)|b_j\rangle\langle b_j|.$$

Now, if (a) $i \neq j$ the duality means $\mathrm{tr}(\sigma_i'\sigma_j) = 0$, and thus

$$\sum_{b_j=0}^{p-1} \exp\left(\frac{2\pi \mathrm{i}}{p} b_j\,\mathrm{tr}(\sigma_i'\sigma_j)\right)|b_j\rangle\langle b_j| = \sum_{b_j=0}^{p-1} |b_j\rangle\langle b_j| = I_j,$$

where the index j means the jth particle;

(b) $i = j$ we have $\mathrm{tr}(\sigma_i'\sigma_i) = 1$ and then,

$$\sum_{b_i=0}^{p-1} \exp\left(\frac{2\pi \mathrm{i}}{p} b_i\,\mathrm{tr}(\sigma_i'\sigma_i)\right)|b_i\rangle\langle b_i| = \sum_{b_i=0}^{p-1} \exp\left(\frac{2\pi \mathrm{i}}{p} b_i\right)|b_i\rangle\langle b_i| = Z_i.$$

Finally, we obtain the factorization

$$Z_{\sigma_i'} = I_1 \otimes \cdots \otimes I_{i-1} \otimes Z_i \otimes I_{i+1} \otimes \cdots I_n,$$

i.e. one Z operator is located in the ith place, and all the other entries are unity.

In particular, making use of an almost self-dual basis (see appendix A),

$$\beta = \sum_{j=1}^n b_j\sigma_j, \qquad \mathrm{tr}(\sigma_i\sigma_j) = q_j\delta_{ij}, \qquad b_j, q_j \in \mathcal{Z}_p, \tag{72}$$

where $q_j \neq 1$ only for a single basis element (say $q_n = q \neq 1$), we have

$$Z_\beta = \otimes \Pi_{j=1}^n Z^{b_j q_j} = Z^{b_1} \ldots Z^{b_{n-1}} Z^{q b_n}. \tag{73}$$

On the other hand, in any almost self-dual basis the X_β operator is a factorized product of single particle X operators (5) in an obvious way. It is clear that

$$X_{\sigma_i} = \sum_{\beta \in GF(d)} |\beta + \sigma_i\rangle\langle\beta| = I_1 \otimes \cdots \otimes I_{i-1} \otimes X_i \otimes I_{i+1} \otimes \cdots I_n,$$

where we use expansion (72) for β, thus

$$X_\beta = \otimes\Pi_{j=1}^{n} X^{b_j}. \tag{74}$$

The above equation is a result of relation (7) and factorization of the finite Fourier transform operator (6) in the almost self-dual basis,

$$F = \otimes\Pi_{j=1}^{n-1} F_j \otimes \tilde{F}_n,$$

where

$$\tilde{F}_n = \frac{1}{\sqrt{p}} \sum_{m,k=0}^{p-1} \omega(qmk)|m\rangle\langle k|.$$

For instance, in the case of $GF(3^2)$ (when the self-dual basis does not exist) the Fourier operator is factorized into $F = F_1 \otimes F_2^\dagger$ in the almost self-dual basis $\{\theta^2, \theta^4\}$, where θ is a root of the irreducible polynomial $x^2 + x + 2 = 0$.

Obviously, in the self-dual basis F is factorized into a product of single particle Fourier operators, $F = \otimes\Pi_{j=1}^{n} F_j$.

Besides, the kernel operator (13) for char $GF(d) \neq 2$, acquires the form

$$\Delta(\alpha, \beta) = \frac{1}{d} \sum_{\gamma,\delta \in GF(d)} \chi(\alpha\delta - \beta\gamma - 2^{-1}\gamma\delta) Z_\gamma X_\delta,$$

and thus can easily be factorized into one-particle operators in any almost self-dual basis. In fact, due to equations (73), (74) and factorization of the generalized character

$$\chi(\alpha\delta) = \Pi_{j=1}^{n} \omega(\alpha_j \delta_j q_j),$$

where $\alpha_j, \delta_j, \in \mathbb{Z}_p$ are coefficients of expansion of α and δ respectively in an almost self-dual basis

$$\alpha = \sum_{j=0}^{p-1} \alpha_j \sigma_j, \qquad \delta = \sum_{j=0}^{p-1} \delta_j \sigma_j,$$

and $\mathrm{tr}\big(\sigma_j^2\big) = q_j = (q-1)\delta_{jn} + 1$. Taking into account (A.2), we have

$$\begin{aligned}\Delta(\alpha, \beta) &= \prod_{i=1}^{n} \left[\frac{1}{p} \sum_{\gamma_i,\delta_i \in GF(d)} \chi((\alpha_i\delta_i - \beta_i\gamma_i - 2^{-1}\gamma_i\delta_i)q_i) Z^{\gamma_i q_i} X^{\delta_i} \right] \\ &= \otimes \prod_{i=1}^{n-1} \Delta(\alpha_i, \beta_i) \otimes \Delta(q\alpha_n, \beta_n).\end{aligned}$$

So that, in any self-dual basis $\Delta(\alpha, \beta) = \otimes\Pi_{i=1}^{n} \Delta(\alpha_i, \beta_i)$.

In the case of a single 'particle' the states of a physical system can be labelled by the elements of the field arranged in some order $(0, \alpha_1, \ldots, \alpha_{p^{n-1}})$ (see previous section). Then, the free Hamiltonian of the system takes on the form

$$H = E_0|0\rangle\langle 0| + E_1|\alpha_1\rangle\langle\alpha_1| + \cdots + E_{p^{n-1}}|\alpha_{p^{n-1}}\rangle\langle\alpha_{p^{n-1}}|,$$

where the energies are arranged in the non-decreasing order: $E_0 \leqslant E_1 \leqslant \cdots \leqslant E_{p^{n-1}}$.

7. Conclusions

In this paper, we have studied an explicit form of the kernel operator (the phase point operator [1, 2]) which maps states of a quantum system of dimension $d = p^n$ into a Wigner function in a discrete phase space. The crucial point in the phase space construction is played by the rotation and displacement operators labelled with elements of $GF(d)$. These operators are explicitly related after imposing condition (46) and allow us to establish a clear correspondence between states in the Hilbert space of the system and lines in the discrete phase space. The structure of the rotation operators is quite different for fields of odd and even characteristic. While for the fields of odd characteristic the rotation operators form a p^n-dimensional Abelian group, the corresponding group in the case of $GF(2^n)$ is of order 2^{2n} and includes both 'rotation' and 'vertical' displacement operators $X_\mu, \mu \in GF(2^n)$. So that although for a particular phase-space construction the group property is not really necessary, different choices of sets of rotation operators lead to different Wigner functions, which is directly connected to the freedom in the election of quantum nets in the Wootters' construction [2]. Such freedom obviously exists also in the case of odd characteristics, which nevertheless can be avoided by fixing the rotation group in a natural way (33).

Acknowledgments

This work is partially supported by the grant 45704 of Consejo Nacional de Ciencia y Tecnologia (CONACyT), Mexico.

Appendix A. Finite fields

A set $\mathcal{L}$ is a commutative *ring* if two binary operations: addition and multiplication (both commutative and associative) are defined.

A *field* F is a commutative ring with division, i.e. for any $a \in F$ there exists $a^{-1} \in F$ so that $a^{-1}a = aa^{-1} = I$ (excluding the zero element). The elements of a field form groups with respect to addition F and multiplication $F^* = F - \{0\}$.

The characteristic of a *finite field* is the smallest integer p, so that $p \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{\text{p times}} = 0$ and it is always a prime number. Any finite field contains a prime subfield $\mathcal{Z}_p$ and has p^n elements, where n is a natural number. Moreover, the finite field containing p^n elements is unique and is usually called a Galois field, $GF(p^n)$. $GF(p^n)$ is an extension of degree n of $\mathcal{Z}_p$, i.e. elements of $GF(p^n)$ can be obtained with $\mathcal{Z}_p$ and all the roots of an *irreducible polynomial* (that is, one which cannot be factorized in $\mathcal{Z}_p$) with coefficients inside $\mathcal{Z}_p$.

The multiplicative group of $GF(p^n) : GF(p^n)^* = GF(p^n) - \{0\}$ is cyclic $\theta^{p^n} = \theta, \theta \in GF(p^n)$. The generators of this group are called *primitive elements* of the field.

A primitive element of $GF(p^n)$ is a root of an irreducible polynomial of degree n over $\mathcal{Z}_p$. This polynomial is called a *minimal polynomial*.

The trace operation

$$\mathrm{tr}(\alpha) = \alpha + \alpha^2 + \cdots + \alpha^{p^{n-1}}$$

maps any field element into an element of the prime field, $\mathrm{tr} : \underset{\alpha}{GF(p^n)} \rightarrow \underset{\mathrm{tr}(\alpha)}{\mathcal{Z}_p}$, and satisfies the property

$$\mathrm{tr}(\alpha_1 + \alpha_2) = \mathrm{tr}(\alpha_1) + \mathrm{tr}(\alpha_2). \tag{A.1}$$

The additive characters are defined as

$$\chi(\alpha) = \exp\left[\frac{2\pi i}{p}\operatorname{tr}(\alpha)\right],$$

and possess two important properties:

$$\chi(\alpha_1 + \alpha_2) = \chi(\alpha_1)\chi(\alpha_2)$$

and

$$\sum_{\alpha\in GF(p^n)} \chi(\alpha) = 0.$$

Any finite field $GF(p^n)$ can be considered as an n-dimensional linear vector space and there is a basis $\{\sigma_j, j = 1, \ldots, n\}$ in this vector space, so that any $\alpha \in GF(p^n), \alpha = \sum_{j=1}^n a_j\sigma_j$ and $a_j \in \mathcal{Z}_p$. Then, for any $f(\alpha)$ one has

$$\sum_{\alpha\in GF(p^n)} f(\alpha) = \sum_{a_1,\ldots,a_n} f(a_1\sigma_1 + \cdots + a_n\sigma_n). \qquad \text{(A.2)}$$

There are several bases, one of which is the *polynomial basis* $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$, where θ is a primitive element of $GF(p^n)$; another one is the *normal basis* $\{\theta, \theta^p, \ldots, \theta^{p^{n-1}}\}$, so one can choose whichever according to the specific problem.

The two bases $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ in the same field are dual if $\operatorname{tr}(\alpha_i\beta_j) = \delta_{ij}$. A basis which is dual to itself is called *self-dual basis*, $\operatorname{tr}(\alpha_i\alpha_j) = \delta_{ij}$.

Example. $GF(2^2)$, the primitive polynomial is $x^2 + x + 1 = 0$, it has the roots $\{\theta, \theta^2\}$. The polynomial basis is $\{1, \theta\}$, whose dual basis is $\{\theta^2, 1\}$:

$$\operatorname{tr}(1\theta^2) = 1, \qquad \operatorname{tr}(11) = 0,$$
$$\operatorname{tr}(\theta\theta^2) = 0, \qquad \operatorname{tr}(\theta 1) = 1.$$

The normal basis $\{\theta, \theta^2\}$ is self-dual:

$$\operatorname{tr}(\theta\theta) = 1, \qquad \operatorname{tr}(\theta\theta^2) = 0,$$
$$\operatorname{tr}(\theta^2\theta) = 0, \qquad \operatorname{tr}(\theta^2\theta^2) = 1.$$

The self-dual basis cannot always be found and the following theorem applies.

Theorem [21]. For every prime power $d = p^n$, there exists an almost self-dual basis of $GF(p^n)$ over $\mathcal{Z}_p$. Moreover, it has a self-dual basis if and only if either p is even or both n and p are odd.

The almost self-dual basis satisfies the properties $\operatorname{tr}(\theta_i\theta_j) = 0$ when $i \neq j$ and $\operatorname{tr}(\theta_i^2) = 1$, with one possible exception. For instance, in the case of $GF(3^2)$ two elements $\{\theta^2, \theta^4\}, \theta$ being a root of the irreducible polynomial $x^2 + x + 2 = 0$, form an almost self-dual basis, i.e.

$$\operatorname{tr}(\theta^2\theta^2) = 1, \qquad \operatorname{tr}(\theta^4\theta^4) = 2, \qquad \operatorname{tr}(\theta^2\theta^4) = 0.$$

Appendix B. Solution of the equation $c_{\kappa+\alpha,\mu}c^*_{\kappa,\mu} = c_{\alpha,\mu}\chi(\mu\alpha\kappa)$ in the $d = 2^n$ case

To solve equation (29) we first fix a basis in the field $GF(2^n)$: $\{\sigma_j, j = 1, \ldots, n\}$, so that any element of the field can be represented as a linear combination

$$\alpha = \sum_{j=1}^n a_j\sigma_j, \qquad a_j \in \mathcal{Z}_2. \qquad \text{(B.1)}$$

Then, we solve the equation (34) $c^2_{\kappa,\mu} = \chi(\kappa^2\mu)$ for the n basis elements $c_{\kappa,\mu}, \kappa = \sigma_1, \ldots, \sigma_n$, assigning in an arbitrary way the signs ± 1 to the square root $\sqrt{\chi(\kappa^2\mu)}$. This means that there exist 2^n different sets of $\{c_{\kappa,\mu}\}$, and thus 2^n different operators V_μ (for a fixed value of μ), which can be precisely parameterized as in equation (30). Once the signs of $c_{\kappa,\mu}$, $\kappa = \sigma_1, \ldots, \sigma_n$, are fixed, the rest of the $2^n - n$ coefficients $c_{\kappa,\mu}$ can be found using expansion (B.1) and relation (29) in the form $c_{\kappa+\alpha,\mu} = c_{\kappa,\mu}c_{\alpha,\mu}\chi(-\mu\alpha\kappa)$ leading to the following result:

$$\begin{aligned} c_{\alpha,\mu} &= c_{a_1\sigma_1+\cdots+a_n\sigma_n,\mu} = c_{a_1\sigma_1,\mu}c_{a_2\sigma_2+\cdots+a_n\sigma_n,\mu}\chi\left(a_1\sigma_1\left(a_2\sigma_2+\cdots+a_n\sigma_n\right)\mu\right) \\ &= \cdots = \chi\left(\mu\sum_{k=1}^{n-1}a_k\sigma_k\sum_{j=k+1}^{n}a_j\sigma_j\right)\Pi_{l=1}^{n}c_{a_l\sigma_l,\mu}, \end{aligned}$$

and $c_{0,\mu} = 1$.

To illustrate how this procedure works let us apply it to the case of $GF(2^2)$. We choose the normal, self-dual, basis $\{\theta, \theta^2\}$ (see appendix A) in $GF(2^2)$, where θ is a root of the primitive polynomial $x^2 + x + 1 = 0$, so that $\theta^3 = \theta + \theta^2$. The solution of equation (34) for, say $\mu = \theta^3 = 1$, is (below we will omit the index μ in the coefficients $c_{\alpha,\mu}$)

$$c_0 = 1, \qquad c_\theta = \pm\mathrm{i}, \qquad c_{\theta^2} = \pm\mathrm{i}.$$

Then, the last coefficient is given by

$$c_{\theta^3} = c_{\theta+\theta^2} = c_\theta c_{\theta^2}\chi\left(1\right) = \left(\pm\mathrm{i}\right)\left(\pm\mathrm{i}\right)\left(1\right),$$

and one can see that there exist 4 different possible operators V_{θ^3}. A similar calculation can be made for the operators V_θ and V_{θ^2}.

It is convenient to fix the positive signs of the coefficients $c_{\kappa,\mu}$ corresponding to the elements of the field basis, i.e. $c_{a_l\sigma_l,\mu} = \sqrt{\chi(a_l^2\sigma_l^2\mu)}$, $l = 1, \ldots, n$, and form the 'first' set of the rotation operators, V_μ with these coefficients. Then, all the other sets of $V_{\mu,\nu}$ can be obtained according to (30).

Once we have the coefficients $c_{\alpha,\mu}$ one can easily obtain the corresponding phase factors for the displacement operator (50). For instance, fixing the 'first' set of rotation operators in the above example as

$$V_\theta = \mathrm{diag}(1, 1, i, -i), \qquad V_{\theta^2} = \mathrm{diag}(1, i, 1, -i), \qquad V_{\theta^3} = \mathrm{diag}(1, i, i, -1), \tag{B.2}$$

we obtain the following phase factors appearing in the displacement operator:

$$\begin{array}{lll} \phi(\theta,\theta) = i, & \phi(\theta,\theta^2) = 1, & \phi(\theta,\theta^3) = i, \\ \phi(\theta^2,\theta) = 1, & \phi(\theta^2,\theta^2) = i, & \phi(\theta^2,\theta^3) = i, \\ \phi(\theta^3,\theta) = -i, & \phi(\theta^3,\theta^2) = -i, & \phi(\theta^3,\theta^3) = -1. \end{array}$$

Another set of rotation operators can be obtained, for instance, by keeping V_θ and V_{θ^2} as in the above and multiplying the operator V_{θ^3} in (B.2) by X_θ:

$$V_\theta = \mathrm{diag}(1, 1, i, -i), \qquad V_{\theta^2} = \mathrm{diag}(1, i, 1, -i), \qquad V_{\theta^3} = \mathrm{diag}(1, -i, i, 1),$$

which leads to some changes in the phases of the displacement operator:

$$\begin{array}{lll} \phi(\theta,\theta) = -i, & \phi(\theta,\theta^2) = 1, & \phi(\theta,\theta^3) = i, \\ \phi(\theta^2,\theta) = 1, & \phi(\theta^2,\theta^2) = i, & \phi(\theta^2,\theta^3) = i, \\ \phi(\theta^3,\theta) = -i, & \phi(\theta^3,\theta^2) = -i, & \phi(\theta^3,\theta^3) = 1. \end{array}$$

Appendix C. Determination of $f(\mu, \mu')$

In practice, the function $f(\mu, \mu')$ is determined by solving the following equation,

$$c_{\alpha,\mu}c_{\alpha,\mu'} = \chi(\alpha f(\mu, \mu'))c_{\alpha,\mu+\mu'}, \tag{C.1}$$

for all values of α belonging to the basis of the field. The rest of the elements of the field do not provide additional information due to (29).

As an example we consider the case of $GF(2^2)$. Following the general procedure, we choose the self-dual basis (θ, θ^2) in the field and fix the rotation operators as in (B.2). Equation (C.1) for $f(\theta, \theta)$ has the form

$$c_{\alpha,\theta}c_{\alpha,\theta} = \chi\left(\alpha f(\theta, \theta)\right)c_{\alpha,0},$$

and for different values of the parameter α we get

$$\alpha = \theta, \qquad 1 \cdot 1 = \chi(\theta f(\theta, \theta))1,$$
$$\alpha = \theta^2, \qquad i \cdot i = \chi(\theta^2 f(\theta, \theta))1,$$

leading to the only possible solution $f(\theta, \theta) = \theta^2$.

Similarly we obtain for the rest of the $f(\mu, \mu')$:

for $f(\theta, \theta^2)$

$$\alpha = \theta, \qquad 1 \cdot i = \chi(\theta f(\theta, \theta^2))i,$$
$$\alpha = \theta^2, \qquad i \cdot 1 = \chi(\theta^2 f(\theta, \theta^2))i,$$

so that $f(\theta, \theta^2) = 0$, and following the same idea we can determine

$$f(\theta, \theta^3) = \theta^2, \qquad f(\theta^2, \theta^2) = \theta, \qquad f(\theta^2, \theta^3) = \theta, \qquad f(\theta^3, \theta^3) = \theta^3.$$

Appendix D. Other symplectic operators

D.1. U operator

In order to introduce another operator [13] with similar properties to V_μ, let us define that two lines are orthogonal if the states corresponding to these lines are related via the Fourier transform

$$|\kappa\rangle \xrightarrow{F} |\widetilde{\kappa}\rangle.$$

Then, there exists an operator $U_\mu|\widetilde{\kappa}\rangle = FV_\mu|\kappa\rangle$ such that its geometrical application rotates the line corresponding to the state $|\kappa\rangle$ (conjugate to $|\widetilde{\kappa}\rangle$), and then transforms the rotated line into an orthogonal one. This operator is obtained from V_μ as

$$U_\mu = FV_\mu F^\dagger = \sum_{\kappa\in GF(d)} c_{-\kappa,\mu}|\kappa\rangle\langle\kappa|, \tag{D.1}$$

so that $U_\mu Z_\alpha U_\mu^\dagger = Z_\alpha$ for all α, μ. The action of U_μ on the operator X_β can be obtained using the operational relation in (D.1) and relation (7)

$$U_\mu X_\beta U_\mu^\dagger = F\left(V_\mu Z_\beta V_\mu^\dagger\right)^\dagger F^\dagger = \exp(-\mathrm{i}\varphi(\beta, \mu))Z_{\mu\beta}^\dagger X_\beta, \tag{D.2}$$

which means that the U-transformation also represents a sort of rotation: operators $U_{\mu'}$ transform eigenstates of the set of displacement operators labelled with points of the ray $\beta = \mu\alpha$

$$\left\{I, Z_{\alpha_1}X_{\mu\alpha_1}, Z_{\alpha_2}X_{\mu\alpha_2}, \ldots\right\} \tag{D.3}$$

to the eigenstates of the set labelled with points of the ray $\beta = (\mu + \mu')^{-1}\alpha$

$$\left\{I, Z_{(1+\mu\mu')\alpha_1} X_{\mu\alpha_1}, Z_{(1+\mu\mu')\alpha_2} X_{\mu\alpha_2}, \ldots\right\}. \tag{D.4}$$

Similarly, as we cannot reach the ray $\alpha = 0$ using V_μ operators, one cannot reach the ray $\beta = 0$ using $U_{\mu'}$ operators. Having both operators $U_{\mu'}$ and V_μ we can transform any ray into any other.

Let us find the Wigner function of one state transformed by V_μ and U_μ operators. For fields of odd characteristic, $p \neq 2$, one can use the explicit form (33) of V_μ and after some algebra we obtain

$$W_{\tilde{\rho}}(\alpha, \beta) = W_\rho(\alpha, \beta - \mu\alpha), \qquad \tilde{\rho} = V_\mu \rho V_\mu^\dagger. \tag{D.5}$$

In the same manner we evaluate the Wigner function of a state transformed by the U_μ operator, $p \neq 2$:

$$W_{\tilde{\rho}}(\alpha, \beta) = W_\rho(\alpha - \mu\beta, \beta), \qquad \tilde{\rho} = U_\mu \rho U_\mu^\dagger. \tag{D.6}$$

In other words, the transformation of a state by the V_μ and/or the U_μ operators leads to a covariant transformation of the Wigner function for the fields of odd characteristics.

D.2. S operator

The last operator which transforms the operators labelled with points of one line into the operators labelled with the points of some other line is the so-called squeezing operator, which in the basis of eigenstates of Z_α operators has the following form:

$$S_\xi = \sum_{\kappa \in GF(p^n)} |\kappa\rangle\langle\xi\kappa|. \tag{D.7}$$

It is easy to see that

$$W_{\tilde{\rho}}(\alpha, \beta) = W_\rho(\xi\alpha, \xi^{-1}\beta), \qquad \tilde{\rho} = S_\xi \rho S_\xi^\dagger.$$

The squeezing operator naturally appears as a result of the consecutive application of V_μ and U_ν:

$$W_{\rho'} = W_{S_\xi \rho S_\xi^\dagger}, \qquad \tilde{\rho} = V_{-\xi(\xi-1)\mu^{-1}} U_{-\xi^{-1}\mu} V_{(\xi-1)\mu^{-1}} U_\mu \rho U_\mu^\dagger V_{(\xi-1)\mu^{-1}}^\dagger U_{-\xi^{-1}\mu}^\dagger V_{-\xi(\xi-1)\mu^{-1}}^\dagger,$$

where μ is an arbitrary element of $GF(p^n)^*$, $p \neq 2$.

References

[1] Wootters W K 1987 *Ann. Phys.* **176** 1
[2] Gibbons K S, Hoffman M J and Wootters W K 2004 *Phys. Rev.* A **70** 062101
[3] Koniorczyk M, Buzek V and Janszky J 2001 *Phys. Rev.* A **64** 034301
[4] Bianucci P, Miquel C, Paz J P and Saraceno M 2002 *Phys. Lett.* A **297** 353
Miquel C, Paz J P and Saraceno M 2002 *Phys. Rev.* A **65** 062309
[5] Paz J P 2002 *Phys. Rev.* A **65** 062311
[6] Paz J P, Roncaglia A J and Saraceno M 2005 *Phys. Rev.* A **72** 012309
[7] Lidl R and Niederreiter H 1986 *Introduction to Finite Fields and their Applications* (Cambridge: Cambridge University Press)
[8] Vourdas A 2005 *J. Phys. A: Math. Gen.* **38** 8453
[9] Pittenger A O and Rubin M H 2005 *J. Phys. A: Math. Gen.* **38** 6005
[10] Klimov A B and Munoz C 2005 *J. Opt. B: Quantum Semiclass. Opt.* **7** S588
[11] Colin S, Corbett J, Durt T and Gross D 2005 *J. Opt. B: Quantum Semiclass. Opt.* **7** S778
[12] Klimov A B, Sánchez-Soto L L and de Guise H 2005 *J. Phys. A Math. Gen.* **38** 2747
[13] Vourdas A 1996 *J. Phys. A: Math. Gen.* **29** 4275
Vourdas A 2003 *J. Phys. A: Math. Gen.* **36** 5645

Vourdas A 2004 *Rep. Prog. Phys.* **67** 267
[14] Galetti D and de Toledo Piza A F R 1988 *Physica* A **149** 267
Hakioglu T 1998 *J. Phys. A: Math. Gen.* **31** 6975
Agam O and Brenner N 1995 *J. Phys. A: Math. Gen.* **28** 1345
Athanasiuyk G G, Floratos E G and Nicolis S 1996 *J. Phys. A: Math. Gen.* **29** 6737
Ellinas D and Floratos E G 1999 *J. Phys. A: Math. Gen.* **32** L63
Leonhardt U 1996 *Phys. Rev.* A **53** 2998
Galetti D 2000 *Ann. Phys.* **249** 454
Galetti D and Ruzzi M 2000 *J. Phys. A: Math. Gen.* **33** 2799
Galetti D and Ruzzi M 1999 *Physica* A **264** 473
Luis A and Perina J 1998 *J. Phys. A: Math. Gen.* **31** 1423
Arguelles A and Dittrich T 2005 *Physica* A **356** 72
[15] Schwinger J 1960 *Proc. Natl Acad. Sci. USA* **46** 893
Schwinger J 1960 *Proc. Natl Acad. Sci. USA* **46** 1401
Schwinger J 1960 *Proc. Natl Acad. Sci. USA* **46** 893
[16] Stratonovich R L 1956 *Sov. Phys.—JETP* **31** 1012
Várilly J C and Gracia-Bondía J M 1989 *Ann. Phys.* **190** 107
[17] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363
[18] Bandyopadhyay S, Boykin P, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512
[19] Saniga M, Planat M and Rosu H 2004 *J. Opt. B: Quantum Semiclass. Opt.* **6** L19
Planat M and Rosu H 2005 *Eur. Phys. J.* D **36** 133
Durt T 2005 *J. Phys. A: Math. Gen.* **38** 5267
[20] Asplund R and Björk G 2001 *Phys. Rev.* A **64** 012106
[21] Jungnickel D 1993 *Finite Fields* (Mannheim: Wissenschaftsverlag)