Introduction to discrete calculus.

Dr. Andrei Klimov. Universidad de Guadalajara, klimov@cencar.udg.mx

Introduction to discrete calculus

When we consider that all the algebraic operations are mod p, p-a prime number, the set of integers $\{0, 1, ..., p-1\}$ form a commutative group with respect to summation and $\{1, ..., p-1\}$ form a group with respect to multiplication.

a) $a \cdot b = c \in Z_p$

b) exists a e neutral element $a \cdot e = e \cdot a = a$,

c) For any a exists inverse elements $a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = e$,

where $\cdot$ means summation or multiplication. Such structure is called an *algebraic field,* which in this case coincides with Z_p .
Let us consider a finite (p-)dimensional Hilbert space $\mathcal{H}$ and choose $\{|n\rangle\}$ as an orthogonal basis, here $n = 0, ..., p-1$. Two basic operators X and Z are introduced as

$$Z|n\rangle = \omega(n)|n\rangle \ \rightarrow \ Z = \sum_{n=0}^{p-1} \omega(n)|n\rangle\langle n|,$$

$$X|n\rangle = |n+1\rangle \ \rightarrow \ X = \sum_{n=0}^{p-1} |n+1\rangle\langle n|, .$$

where

$$\omega = e^{\frac{2\pi i}{p}}, \quad \omega(n) = \omega^n, \quad \sum_{n=0}^{p-1} \omega(nk) = p\delta_{k,0}.$$

Due to the above definitions it is easy to see that

$$ZX|n\rangle = \omega(n+1)|n+1\rangle, \quad XZ|n\rangle = \omega(n)|n+1\rangle,$$

so that

$$ZX = \omega XZ,$$

and $\{Z, X\}$ form the so-called "generalized Pauli group". It is clear that $Z^p = X^p = I$, i.e. X, Z are cyclic operators.

There exists another (dual) basis $\{|\tilde{n}\rangle\}$ where Z acts displacing by one any basis state

$$Z|\tilde{n}\rangle = |\widetilde{n+1}\rangle. \tag{1}$$

In order to get an explicit expression for the states $|\tilde{n}\rangle$ in terms of the basis $\{|n\rangle\}$, we will write

$$|\tilde{n}\rangle = \sum_{n=0}^{p-1} a_{n,k}|k\rangle$$

and applying Z is possible to find an equation for the coeficients $a_{n,k}$, this application is obvious

$$Z|\tilde{n}\rangle = \sum_{n=0}^{p-1} \omega(k) a_{n,k}|k\rangle$$

and the expansion of the right-hand side of (1) is rewritten as

$$|\widetilde{n+1}\rangle = \sum_{n=0}^{p-1} a_{n+1,k}|k\rangle,$$

obtaining the equation $a_{n+1,k} = \omega(k)a_{n,k}$. The solution has the form $a_{n,k} = c\omega(nk)$, getting the value of c from the normalization condition

$$|\tilde{n}\rangle = c\sum_{k=0}^{p-1} \omega(nk)|k\rangle \rightarrow \langle\tilde{n}|\tilde{n}\rangle = 1 \rightarrow c = \frac{1}{\sqrt{p}}.$$

The operator which maps from the basis $|n\rangle$ into the dual basis $|\tilde{n}\rangle$,

$$|\tilde{n}\rangle = F|n\rangle, \tag{2}$$

is the finite Fourier transform

$$F = \frac{1}{\sqrt{p}} \sum_{k,n=0}^{p-1} \omega(nk)|n\rangle\langle k|$$

and it satisfies the unitarity property $FF^\dagger = F^\dagger F = I$.

When $p \neq 2$ the square of this operator is

$$F^2 = \frac{1}{p} \sum_{k,n,k'=0}^{p-1} \omega(k(n+k'))|n\rangle\langle k'| = \sum_{k}^{p-1} |-k\rangle\langle k| = P,$$

here P is the parity operator, which leads to

$$F^4 = P^2 = I, \tag{3}$$

otherwise $(p=2)$ $F^2 = I$.

Here, the abcence of the parity operator is a consequence of a structural difference between $p=2$ and odd primes. This difference will appear several times from now on along the whole articule, we will point out whenever it needs.

The action of X in the dual basis is

$$X|\tilde{n}\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \omega((k-1)n)|k\rangle = \omega^*(n)|\tilde{n}\rangle,$$

i.e. the operator X is diagonal is diagonal in the dual basis $|\tilde{n}\rangle$ and its eigenvalues are related to the eigenvalues of the Z operator through conjugation. Using (2) we can find the relation between X and Z via the finite Fourier transform, let us consider the odd prime case, firstly,

$$\begin{aligned} X &= F \sum_{n=0}^{p-1} \omega(-n)|n\rangle\langle n|F^\dagger \\ &= FP \sum_{n=0}^{p-1} \omega(n)|n\rangle\langle n|PF^\dagger, \end{aligned}$$

considering (3)

$$X = F^\dagger Z F. \tag{4}$$

Due to both $\omega(-n) = \omega(n)$ and $F^2 = I$ when $p=2$, the result (4) has the same form for all the primes.

The operators Z and X satisfy the following important properties:

$$Tr(X^n X^{\dagger m}) = p\delta_{mn}, \quad Tr(Z^n Z^{\dagger m}) = p\delta_{mn}, \quad Tr(Z^n X^m) = p\delta_{m0}\delta_{n0}.$$

The collection of operators $D(\alpha,\beta) = \phi(\alpha,\beta)Z^\alpha X^\beta$, where ϕ is a phase, form an operational basis in $\mathcal{H}$ and any operator $\hat{f}$ can be expanded as

$$\hat{f} = \sum_{\alpha,\beta=0}^{p-1} f_{\alpha,\beta} D(\alpha,\beta). \tag{5}$$

These operators are orthogonal

$$\mathrm{Tr}\left(D(\alpha,\beta)D^\dagger(\alpha',\beta')\right) = p\delta_{\alpha,\alpha'}\delta_{\beta,\beta'},$$

helped with this property, the coeficients in (5) can be found as

$$f_{\alpha,\beta} = \frac{1}{p}\mathrm{Tr}\left(\hat{f}D^\dagger(\alpha,\beta)\right).$$

This means that we can map $\hat{f} \in \mathrm{Op}(\mathcal{H})$ into $f_{\alpha,\beta}$ which is a function of discrete variables defined on a discrete 2-dim space M. The coordinates (α,β) in M are given by the powers of Z and X, respectively. Due to the periodicity of Z and X the space M is diffeomorphic to a bidimensional discrete torus. The action of the operator $D(\alpha',\beta')$ on an arbitrary point (α,β) on the manifold is just the displacement $(\alpha+\alpha',\beta+\beta')$, for this reason $D(\alpha',\beta')$ is called a *displacement operator*.

To ilustrate how this mapping is performed let us get the discrete representation of $|k\rangle$, it is

$$\begin{aligned} |k\rangle\langle k| \leftrightarrow f_{\alpha,\beta}(k) &= \frac{1}{p}\mathrm{Tr}\left[|k\rangle\langle k|D^\dagger(\alpha,\beta)\right] = \\ &= \frac{1}{p}\phi^*(\alpha,\beta)\omega(-k\alpha)\delta_{\beta,0}, \end{aligned}$$

as a disadvantage of that result is its non-reality.

A problem which arises using (5) is that it is not covariant under the application of the displacement operator

$$\tilde{f} = D(\gamma,\delta)fD^\dagger(\gamma,\beta) = \sum_{\alpha,\beta=0}^{p-1} f_{\alpha,\beta}\omega(\beta\gamma-\alpha\delta)D(\alpha,\beta).$$

But it is easy to solve and a covariant operator is given by the following construction

$$\Delta(\alpha,\beta) = \frac{1}{p}\sum_{\gamma,\delta=0}^{p-1} \omega(\alpha\delta-\beta\gamma) D(\gamma,\delta), \tag{6}$$

this operator also satisfies an orthogonality relation

$$\mathrm{Tr}\left(\Delta(\alpha,\beta)\Delta^{\dagger}(\alpha',\beta')\right) = p\delta_{\alpha,\alpha'}\delta_{\beta,\beta'}.$$

It means that (6) (which we will call kernel) forms an operational basis, as well,

$$f = \sum_{\alpha,\beta=0}^{p-1} W_f(\alpha,\beta)\Delta(\alpha,\beta) \leftrightarrow W_f(\alpha,\beta) = \frac{1}{p}\mathrm{Tr}\left(\hat{f}\Delta(\alpha,\beta)\right). \tag{7}$$

Let us impose the condition $f^{\dagger} \leftrightarrow W_f^*(\alpha,\beta)$ so

$$f^{\dagger} = \sum_{\alpha,\beta=0}^{p-1} W_f^*(\alpha,\beta)\Delta^{\dagger}(\alpha,\beta)$$

therefore $\Delta = \Delta^{\dagger}$, i.e. Δ has to be a Hermitian operator. This also gives us a phase condition

$$\Delta^{\dagger} = \frac{1}{p}\sum_{\gamma,\delta=0}^{p-1} \omega(\alpha\delta-\beta\gamma)\phi^*(-\gamma,-\delta)\omega(-\gamma\delta)Z^{\gamma}X^{\delta},$$

so

$$\phi^*(-\gamma,-\delta)\omega(-\gamma\delta) = \phi(\gamma,\delta). \tag{8}$$

A particular solution of (8) is

$$\phi(\gamma,\delta) = \omega(-2^{-1}\gamma\delta),$$

for odd primes and, for $p=2$,

$$\phi(\gamma,\delta) = (\pm i)^{-\gamma\delta}.$$

As we asked before for, this operator is covariant

$$D(\mu,\nu)\Delta(\alpha,\beta)D^{\dagger}(\mu,\nu) = \Delta(\alpha+\mu,\beta+\nu).$$

The obvious consecuence of the covariance property, and the motivation behind, is that the symbol of a transformed operator

$$\hat{f} = D(\mu,\nu) f D^{\dagger}(\mu,\nu),$$

has the form

$$\begin{aligned} W_{\hat{f}}(\alpha,\beta) &= \frac{1}{p}\mathrm{Tr}(D(\mu,\nu) f D^{\dagger}(\mu,\nu)\Delta(\alpha,\beta)) \\ &= W_f(\alpha-\mu,\beta-\nu). \end{aligned}$$

The normalization condition for (6) is immediately obtained

$$\mathrm{Tr}\Delta(\alpha,\beta) = \frac{1}{p}\sum_{\gamma,\delta=0}^{p-1}\omega(\alpha\delta-\gamma\beta)\phi(\gamma,\delta)\mathrm{Tr}(Z^{\gamma}X^{\delta}) = 1$$

because $\phi(0,0)=1$ for any prime p. This result leads to

$$\mathrm{Tr} f = \sum_{\alpha,\beta=0}^{p-1} W_f(\alpha,\beta).$$

Note that if

$$f = \sum_{\alpha,\beta=0}^{p-1} f_{\alpha,\beta} D(\alpha,\beta),$$

then the symbol of the operator f can be obtained using the coeficients of the operational expansion

$$\begin{aligned} W_f(\alpha,\beta) &= \frac{1}{p}\sum_{\mu,\nu=0}^{p-1} f_{\mu,\nu}\mathrm{Tr}\left(D(\mu,\nu)\Delta(\alpha,\beta)\right) \\ &= \sum_{\mu,\nu=0} f_{\mu,\nu}\omega(-\alpha\nu+\beta\mu). \end{aligned} \tag{9}$$

The trace condition for the multiplication of two given operators is

$$\mathrm{Tr}(fg) = p\sum_{\alpha,\beta=0}^{p-1} W_f(\alpha,\beta) W_g(\alpha,\beta).$$

A convenient representation of (6) for several calculations is

$$\Delta(\alpha,\beta) = \frac{1}{p} D(\alpha,\beta) \sum_{\gamma,\delta=0}^{p-1} D(\gamma,\delta) D^{\dagger}(\alpha,\beta).$$

As an interesting property of the displacement operator we can point out that the equally weighted summation over the whole set of themselves results in the parity operator

$$\frac{1}{p} \sum_{\gamma,\delta=0}^{p-1} D(\gamma,\delta) = \frac{1}{p} \sum_{k=0}^{p-1} \sum_{\gamma,\delta=0}^{p-1} \omega((k+2^{-1}\delta)\gamma) |k+\delta\rangle\langle k| = P,$$

this result is obtained for $p \neq 2$, actually.

To get a better idea about the Wigner function let us see two examples. The Wigner fuction corresponding to the state $|n\rangle$ has the form

$$\begin{aligned} W_{|n\rangle\langle n|} &= \frac{1}{p} \sum_{\gamma,\delta=0}^{p-1} \omega(\alpha\delta - \beta\gamma) \mathrm{Tr}\left(|k\rangle\langle k| D(\gamma,\delta)\right) \\ &= \frac{1}{p} \sum_{\gamma,\delta=0}^{p-1} \omega(\alpha\delta - \beta\gamma) \phi(\gamma,0) \omega(n\gamma) \delta_{\delta,0} = \delta_{\beta,n}; \end{aligned}$$

it is the line $\beta = n$. The second example is the symbol corresponding to Z,

$$\begin{aligned} W_Z &= \frac{1}{p} \sum_{\gamma,\delta=0}^{p-1} \omega(\alpha\delta - \beta\gamma) \mathrm{Tr}(Z D(\gamma,\delta)) \\ &= \sum_{\gamma,\delta=0}^{p-1} \omega(\alpha\delta - \beta\gamma) \delta_{\delta,0} \delta_{\gamma,-1} = \omega(\beta), \end{aligned}$$

this symbol depends only on β.

Discrete phase space geometry

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

$$a\alpha + b\beta = c,$$

where $a, b, c \in Z_p$ are fixed, form a line. Moreover, two lines

$$\begin{aligned} a\alpha + b\beta &= c \\ a'\alpha + b'\beta &= c', \end{aligned}$$

with given $a, b, c, a', b', c' \in Z_p$, are called parallel if they have no common points and it implies the relation among the coefficients

$$\frac{b}{a} = \frac{b'}{a'} \rightarrow ba' = ab'.$$

Also, if the lines are not parallel they cross each other in a single point and its coordinates are

$$\alpha = \frac{c' - b'b^{-1}c}{a' - ab'b^{-1}}, \quad \beta = \frac{c' - a'a^{-1}c}{b' - a'a^{-1}b}.$$

It is called *ray* a line which pass over the origin and its equation has the form

$$\beta = m\alpha, \quad \text{or} \quad \alpha = 0.$$

Of course, there are $p-1$ parallel lines to each one of the $p+1$ rays, therefore the total number of lines is $p(p+1)$. The collection of p parallel lines is called *foliation*.

Displacement in the discrete phase space

Consider a ray λ_m: $\beta = m\alpha$ (or $\alpha = 0$): $(\alpha, m\alpha)$ or $(0, \beta)$ and let us label $D(\alpha, \beta)$ using the points of this ray: $D(\alpha, m\alpha)$ or $D(0, \beta)$. Observe that $[D(\alpha, m\alpha), D(\alpha', m\alpha')] = 0$, i.e. the displacement operators corresponding to the same ray commute. Let us associate the ray λ_m with the eigenstates of $D(\alpha, m\alpha)$, m is fixed.

To show how these operators are, the $\mathcal{Z}_3$ case is written explicitly for all the possible rays

$$\begin{aligned} \beta = 0 &\rightarrow Z, Z^2 \\ \beta = \alpha &\rightarrow ZX, Z^2X^2 \\ \beta = 2\alpha &\rightarrow ZX^2, Z^2X^4 \\ \alpha = 0 &\rightarrow X, X^2. \end{aligned}$$

The set $\{Z^{\alpha}X^{m\alpha}\}$ with fixed m has p different eigenvectors $|\psi_m^n\rangle$, it means

$$D(\alpha, m\alpha)|\psi_m^0\rangle = e^{i\xi_m^0}|\psi_m^0\rangle,$$

where $|\psi_m^0\rangle$ is the state associated with the ray λ_m. Let us define $D(\gamma,\delta)|\psi_m^0\rangle = |\Psi_m\rangle$, observe that

$$\begin{aligned} D(\alpha, m\alpha)|\Psi_m\rangle &= \omega(\alpha\delta - m\alpha\gamma)e^{i\xi_m^0}D(\gamma,\delta)|\psi_m^0\rangle \\ &= \omega(\alpha(\delta - m\gamma))e^{i\xi_m^0}|\Psi_m\rangle, \end{aligned}$$

this means that $|\Psi_m\rangle$ is an eigenstate of $D(\alpha, m\alpha)$ with eigenvalue $\omega(n\alpha)e^{i\xi_m^0}$, here $n = \delta - m\gamma$. So, there are p displacement operators $D(\gamma, m\gamma + n)$ for which $\omega(n\alpha)$ has the same value because m and n are fixed. This displacement operator can be divided into two parts, the first one is the displacement operator associated with some ray and the second one corresponds to X^n,

$$D(\gamma, m\gamma + n) = \omega(-2^{-1}\gamma n)D(\gamma, m\gamma)X^n.$$

Note that the operators $D(\gamma, m\gamma + n)$ are labeled with all the points in the line $\beta = m\alpha + n$, which is parallel to the ray $\beta = m\alpha$. Now, we can define the state

$$|\psi_m^n\rangle = X^n|\psi_m^0\rangle,$$

we already know that the state $|\psi_m^0\rangle$ is put in correspondence to the ray $\beta = m\alpha$, while $|\psi_m^n\rangle$ is associated with the line $\beta = m\alpha + n$, the application of the displacement operator on $|\psi_m^n\rangle$ is given by (**??**). As an additional property of those states we can check that the scalar product of two states with indeces belonging to the same foliation is

$$\langle\psi_m^n|\psi_m^{n'}\rangle = \delta_{n,n'},$$

i.e. they are orthonormal.

Rotations in the phase space

Let us introduce the operator V acording to the following conditions

$$VZ^{\alpha}V^{\dagger} = \varphi Z^{\alpha}X^{\alpha}, \tag{10}$$

where φ is a phase factor which will be determined below and

$$[V, X] = 0. \tag{11}$$

Due to (11) V is diagonal in the basis $\{|\tilde{n}\rangle\}$, it means

$$V = \sum_{n=0}^{p-1} c_n |\widetilde{n}\rangle\langle\widetilde{n}|. \tag{12}$$

We have to determine the coeficients c_n, in order to get them, let us make use of (12) to calculate explicitly the right-hand side of (10) in $\{|\tilde{n}\rangle\}$

$$\begin{aligned} VZ^\alpha V^\dagger &= \sum_{n,n'=0}^{p-1} c_{n'} c_n^* |\widetilde{n}'\rangle\langle\widetilde{n}'|Z^\alpha|\widetilde{n}\rangle\langle\widetilde{n}| \\ &= \sum_{n=0}^{p-1} c_{n+\alpha} c_n^* |\widetilde{n+\alpha}\rangle\langle\widetilde{n}|, \end{aligned}$$

with $c_0 = 1$. The operators at the left-hand side of (10) written in the same basis as before have the form

$$Z^\alpha X^\alpha = Z^\alpha X^\alpha \sum_{n=0}^{p-1} |\widetilde{n}\rangle\langle\widetilde{n}| = \sum_{n=0}^{p-1} \omega(-n\alpha)|\widetilde{n+\alpha}\rangle\langle\widetilde{n}|,$$

leading to an equation for c_n

$$c_{n+\alpha} c_n^* = \varphi\omega(-n\alpha), \to |c_n|^2 = 1. \tag{13}$$

To solve this we have to separate the equation into two cases, when $p \neq 2$ a particular solution to this equation is

$$c_n = \omega(-2^{-1}n^2), \quad c_\alpha = \varphi = \omega(-2^{-1}\alpha^2)$$

and finally we can write

$$V = \sum_{n=0}^{p-1} \omega(-2^{-1}n^2)|\widetilde{n}\rangle\langle\widetilde{n}| \to VZ^\alpha V^\dagger = \omega(-2^{-1}\alpha^2)Z^\alpha X^\alpha.$$

According to that we get

$$V^m Z^\alpha (V^\dagger)^m = \omega(-2^{-1}m\alpha^2)Z^\alpha X^{m\alpha}. \tag{14}$$

From the geometric point of view powers of V generate a β component from the point $(\alpha, 0)$

$$V^m : (\alpha, 0) \to (\alpha, m\alpha) : \lambda_0 \to \lambda_m,$$

it means that the action of V^m produces rotations from one ray to another one.

If $p = 2$ the equation has no modification but because there is no 2^{-1} we have to write the solution in a different manner

$$c_{n+1}c_n^* = \varphi\omega(-n), \quad c_0 = 1, \quad c_1 = \varphi = \pm i,$$

and (10) reads

$$VZV^\dagger = \left\| \begin{matrix} 1 & 0 \\ 0 & i \end{matrix} \right\| Z \left\| \begin{matrix} 1 & 0 \\ 0 & -i \end{matrix} \right\| = iZX.$$

Easily, we can check that $V^p = I$ is a cyclic group, therefore we cannot reach $(0, \beta)$ from $(\alpha, 0)$. Anyhow, we already know the solution and it is performed through the Fourier transform $X^\alpha = F^\dagger Z^\alpha F$, i.e. $|\widetilde{n}\rangle = F|n\rangle$ as it was defined at (2).
Now, let us see the action of V in the Hilbert space

$$\begin{aligned} V|\psi_m^n\rangle &\sim VD(\alpha, m\alpha)V^\dagger V|\psi_m^n\rangle \\ &= \omega(-2^{-1}\,(m+1)\,\alpha^2)Z^\alpha X^{(m+1)\alpha}V|\psi_m^n\rangle, \end{aligned}$$

so then

$$D(\alpha, (m+1)\alpha)[V|\psi_m^n\rangle] = \omega(n\alpha)e^{i\xi_m^0}[V|\psi_m^n\rangle],$$

now we can associate the states $V|\psi_m^n\rangle$ to the states of the foliation where the ray $\beta = (m+1)\,\alpha$ belongs to. As an ilustration the aplication of V^2 on the ray λ_0 gives

$$\underbrace{\lambda_0 \xrightarrow{V} \lambda_1 \xrightarrow{V} \lambda_2}_{V^2},$$

so V^m maps from the ray λ_0 into the ray λ_m, for this reason it represents a rotation.

To introduce another operator with rotation properties similar to V, let us define two lines to be orthogonal if the states corresponding to these ones are related via the Fourier transform

$$|n\rangle \xrightarrow{F} F|n\rangle,$$

there exists an operator $U|\widetilde{n}\rangle = FV|n\rangle$ so its application rotates the state $|n\rangle$ (dual to $|\widetilde{n}\rangle$) and transforms this rotated line into an orthogonal one. This operator can be obtained from V as

$$U = FVF^{\dagger} = \sum_{k=0}^{p-1} c_{-n}|n\rangle\langle n|, \tag{15}$$

of course, $UZU^{\dagger} = Z$. The action of U on the operator X can be obtained using the operational relation in (15) and the relation (4)

$$UXU^{\dagger} = F(VZV^{\dagger})^{\dagger}F^{\dagger} = \varphi^{*}Z^{\dagger}X, \tag{16}$$

so

$$UZ^{\alpha}X^{m\alpha}U^{\dagger} \sim Z^{(1-m)\alpha}X^{m\alpha},$$

and this operator changes the slope of the original ray to give another one

$$\beta = m\alpha \xrightarrow{U} (1-m)\beta = m\alpha,$$

this transformation also represents rotations. This formula reminds us of the imposibility to reach the ray $\alpha = 0$ through V, with U this problem disappears but it cannot reach the ray $\beta = 0$. With both U and V we can tranform from any ray to any other.

A general picture

Let us associate the ray λ_0 (it is the set of all the points $(\alpha, 0)$) with the eigenstate of the operator Z^{α}, so that all the eigenvalues are 1, it is unique and corresponds to the ground state $Z^{\alpha}|0\rangle = |0\rangle$. In a similar way, the states $|n\rangle = X^{n}|0\rangle$ are associated with the parallel lines $\beta = n$ on the phase space. The ray $\lambda_m \leftrightarrow \beta = m\alpha$ corresponds to the state $V^{m}|0\rangle = |\psi_m^0\rangle$, so that all the eigenvalues of $D(\alpha, m\alpha)$ are 1. Finally, gluing last both associations, $|\psi_m^n\rangle = X^{n}|\psi_m^0\rangle$ and the line $\beta = m\alpha + n$ is in conection.
The Wigner function of the state $|\psi_m^n\rangle$ is calculated quite easy. The commutation between X and V allows us to treat the application of each operator independently. The covariance property of the Wigner function gives

$$\begin{aligned} W_{|\psi_0^n\rangle\langle\psi_0^n|}(\alpha,\beta) &= W_{X^n|0\rangle\langle 0|(X^{\dagger})^n}(\alpha,\beta) \\ &= W_{|0\rangle\langle 0|}(\alpha,\beta-n) = \delta_{\beta,n}, \end{aligned}$$

and

$$W_{|\psi_m^0\rangle\langle\psi_m^0|}(\alpha,\beta) = \frac{1}{p}\sum_{\gamma,\delta=0}^{p-1}\omega(\alpha\delta - \beta\gamma)\phi(\gamma,\delta)\omega(2^{-1}m\gamma^2)\langle 0|Z^\gamma X^{\delta - m\gamma}|0\rangle = \delta_{\beta,m\alpha}.$$

This means that the Wigner function of $|\psi_m^n\rangle$ has the form of the line $\beta = m\alpha + n$, precisely.

0.1. Mutually unbiased bases

When the inner product of basis elements of two different bases has the value

$$|\langle\psi_{m'}^{n'}|\psi_m^n\rangle| = \frac{1}{\sqrt{p}}, \tag{17}$$

we say that those bases are mutually unbiased.

Here we show that the bases associated to different foliations are mutually unbiased, and for this reason, the rotations over the discrete phase space become an important issue in this task.

The inner product (17) can be rewritten as

$$\langle 0|(V^\dagger)^m(X^\dagger)^n X^{n'} V^{m'}|0\rangle \tag{18}$$

due to V and X commute, and as a consequence, their powers, as well, the above equation gets the form

$$\langle 0|X^{n'-n}V^{m'-m}|0\rangle = \sum_{k=0}^{p-1} c_k^{m'-m}\langle n-n'|\tilde{k}\rangle\langle\tilde{k}|0\rangle,$$

considering that $\langle n-n'|\tilde{k}\rangle = \omega(k(n-n'))/\sqrt{p}$ and $\langle\tilde{k}|0\rangle = 1/\sqrt{p}$, (18) gets the form

$$\langle 0|(V^\dagger)^m(X^\dagger)^n X^{n'} V^{m'}|0\rangle = \frac{1}{p}\sum_{k=0}^{p-1} c_k^{m'-m}\omega(k(n-n')).$$

Let us introduce the definition

$$\Psi_{m,m'}^{n,n'} \equiv \sum_{k=0}^{p-1} c_k^{m'-m}\omega(k(n-n'))$$

the square of the absolute value of $\Psi^{n,n'}_{m,m'}$ can be calculated easily

$$|\Psi^{n,n'}_{m,m'}|^2 = \sum_{k,k'=0}^{p-1} c_k^{m'-m} c_{k'}^{*m'-m} \omega((k-k')(n-n')),$$

changing the index $k - k' = l$, the above formula is rewritten as

$$\sum_{k',l=0}^{p-1} c_{k'+l}^{m'-m} c_{k'}^{*m'-m} \omega(l(n-n')),$$

substituting (13)

$$\sum_{k',l=0}^{p-1} \varphi^{m-m'}(l)\omega(-lk'(m-m'))\omega(l(n-n'))$$
$$= \left\{ \begin{array}{cc} p^2 \delta_{n,n'} & m = m' \\ p\sum_{l=0}^{p-1} \varphi^{m-m'}(l)\omega(l(n-n'))\delta_{l,0} & m \neq m' \end{array} \right. ,$$

giving the two possible results

$$\frac{1}{p^2}|\Psi^{n,n'}_{m,m'}|^2 = \left\{ \begin{array}{cc} \delta_{n,n'} & m = m' \\ 1/p & m \neq m' \end{array} \right.$$

the first one corresponds to the inner product of states belonging to the same foliation, i.e. same basis, and in the second one we can observe that different foliations correspond to different mutually unbiased bases (MUB).

Reconstruction procedure

Let us calculate the average of the density matrix on the state corresponding to the line $\beta = m\alpha + n$

$$\langle \psi_m^n | \rho | \psi_m^n \rangle = \langle 0 | (V^\dagger)^m (X^\dagger)^n \rho X^n V^m | 0 \rangle,$$

using the expansion (7) for the density matrix and applying (14) we rewrite the above expression as

$$\frac{1}{p}\sum_{p,q=0}^{p-1} W(p,q) \sum_{\gamma,\delta=0}^{p-1} \omega(p\delta - q\gamma)\omega(-2^{-1}\gamma\delta)$$
$$\times \omega(-2^{-1}m\gamma^2)\langle n | Z^\gamma X^{\delta - m\gamma} | n \rangle,$$

as we have done before, we are considering the odd prime case. Taking into account that

$$\langle n|Z^{\gamma}X^{\delta-m\gamma}|n\rangle = \omega\left(\gamma\right)\delta_{m\gamma,\delta}$$

and after few algebra we get

$$\begin{aligned} & \frac{1}{p}\sum_{p,q=0}^{p-1} W(p,q)\sum_{\gamma=0}^{p-1}\omega((mp-q)\,\gamma)\omega\left(n\gamma\right) \\ = & \sum_{p,q=0}^{p-1} W(p,q)\delta_{q,mp+n}. \end{aligned}$$

This means that

$$\langle\psi_m^n|\rho|\psi_m^n\rangle = \sum_{\alpha,\beta=0}^{p-1} W(\alpha,\beta)\delta_{\beta,m\alpha+n},$$

which is a general requirement for the Wigner function. It still needs to be proved the same result for the line $\alpha = 0$, it can be done using the dual basis

$$\begin{aligned} \langle\tilde{l}|\rho|\tilde{l}\rangle &= \langle l|F^{\dagger}\rho F|l\rangle \\ &= \frac{1}{p}\sum_{\alpha,\beta=0}^{p-1} W(\alpha,\beta)\sum_{\gamma,\delta=0}^{p-1}\omega(\alpha\delta-\beta\gamma)\phi(\gamma,\delta)\langle l|X^{\gamma}Z^{-\delta}|l\rangle, \end{aligned}$$

after few algebra, the average value is

$$\langle\tilde{l}|\rho|\tilde{l}\rangle = \sum_{\alpha,\beta=0}^{p-1} W(\alpha,\beta)\delta_{\alpha,l}.$$

The summation of the values of the Wigner function along a line gives the probability that the system will be found to be in the state associated to this line, indeed.

Let us call the average $\langle\psi_m^n|\rho|\psi_m^n\rangle = f(m,n)$ tomogram, and recall that

$$f(m,n) = \frac{1}{p}\sum_{\alpha,\beta=0}^{p-1} W(\alpha,\beta)\delta_{\beta,m\alpha+n} = \frac{1}{p}\sum_{\alpha=0}^{p-1} W(\alpha,m\alpha+n)$$

applying the relation (9) to the density matrix, the right-hand side of the above formula is changed into

$$\sum_{m',n'=0}^{p-1} \rho_{m',n'}\omega(nm')\delta_{n',mm'} = \sum_{m'=0}^{p-1} \rho_{m',m'm}\omega(nm'),$$

finally,

$$f(m,n) = \sum_{m'=0}^{p-1} \rho_{m',m'm}\omega(nm').$$

Written in this form it is now possible to invert the formula in order to get the elements of the density matrix. Multiplying both sides of (**??**) by $\omega\,(-nk)$ and adding over the whole set Z_p

$$\sum_{m',n=0}^{p-1} \rho_{m',m'm}\omega(n(m'-k)) = p\sum_{m'=0}^{p-1} \rho_{m',m'm}\delta_{m',k} = \sum_{n=0}^{p-1} f(m,n)\omega(-kn), \quad (19)$$

we get the desired elements

$$\rho_{k,km} = \frac{1}{p}\sum_{n=0}^{p-1} f(m,n)\omega(-kn),$$

or, changing the second index, in another form

$$\rho_{k,l} = \frac{1}{p}\sum_{n=0}^{p-1} f(lk^{-1},n)\omega(-kn),$$

with $k \neq 0$. Following this recipe almost all the elements of the density matrix can be reconstructed, the elements $\beta_{0,l}$ are not reached.
To reconstruct $\beta_{0,l}$ we have to measure the element

$$f\,(l) = \langle\tilde{l}|\rho|\tilde{l}\rangle = \langle l|F^{\dagger}\rho F|l\rangle = \frac{1}{p}\sum_{\alpha,\beta=0}^{p-1} W(\alpha,\beta)\delta_{\alpha,l},$$

applying (9) and after few algebra

$$f\,(l) = \sum_{n'=0}^{p-1} \rho_{0,n'}\omega(-ln');$$

following a similar procedure than above (19) we obtain the left elements

$$\rho_{0,n} = \frac{1}{p} \sum_{k=0}^{p-1} f(k)\omega(kn).$$

This procedure allows us to get the complete density matrix information from different averages which are available due to some experiments.