

1 Finite fields

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

The simplest example of a ring is a set of natural numbers $\{0, 1, \dots, N - 1\} = \mathcal{Z}_N$, where the algebraic operations are taken by mod N .

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).

Elements of a field form commutative (abelian) groups with respect to addition F and multiplication $F^* = F - \{0\}$.

The characteristic of a *finite field* is the smallest integer p , so that

$$p \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{p \text{ times}} = 0$$

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.

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* (it cannot be factorized in \mathcal{Z}_p) with coefficients in \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*.

Example of non prime fields let us consider the roots of the following irreducible on \mathcal{Z}_2 polynomial:

$$x^2 + x + 1 = 0,$$

then, if θ is a root of this polynomial, then the elements

$$\{0, 1, \theta, \theta^2 = \theta + 1 = \theta^{-1}\}$$

satisfy the following summation and multiplication rules

	1	θ	θ^{-1}
1	1	θ	θ^{-1}
α	α	θ^{-1}	1
θ^{-1}	θ^{-1}	1	θ

Multiplication table

	0	1	θ	θ^{-1}
0	0	1	α	θ^{-1}
1	1	0	θ^{-1}	θ
θ	θ	θ^{-1}	0	1
θ^{-1}	θ^{-1}	θ	1	0

Summation table

and form the finite field $GF(2^2)$; the element θ is the generator of the multiplicative group $GF(2^2)^*$.

One should be careful with factorization of polynomials over finite fields, say the polynomial $x^2 + 1$ is not irreducible over Z_2 :

$$x^2 + 1 = (x + 1)(x + 1).$$

The map $\alpha \rightarrow \alpha^p$, where $\alpha \in GF(p^n)$ is a linear automorphism of $GF(p^n)$. $(\alpha + \beta)^p = \alpha^p + \beta^p$, $(\alpha\beta)^p = \alpha^p\beta^p$, which is called Frobenius automorphism:

$$\sigma^k(\alpha) = \alpha^{p^k}.$$

The elements of the prime field are invariant under action of the Frobenius automorphism.

The trace operation

$$\text{tr}(\alpha) = \alpha + \alpha^2 + \dots + \alpha^{p^{n-1}} = \sum_{k=0}^{n-1} \sigma^k(\alpha), \quad (1)$$

maps any field element into an element of the prime field,

$$\text{tr} : \underset{\alpha}{GF(p^n)} \rightarrow \underset{\text{tr}(\alpha)}{\mathcal{Z}_p},$$

(and thus, leaves the elements of the prime field invariant) and satisfies the property

$$\text{tr}(\alpha_1 + \alpha_2) = \text{tr}(\alpha_1) + \text{tr}(\alpha_2). \quad (2)$$

In the above example of $GF(2^2)$ we in particular obtain:

$$\begin{aligned} \text{tr}(\theta) &= \theta + \theta^2 = \theta + \theta + 1 = 1, \\ \text{tr}(\theta^2) &= \theta^2 + \theta^4 = (\theta + 1) + \theta = 1, \\ \text{tr}(\theta^3) &= \text{tr}(1) = 1 + 1 = 0, \\ \text{tr}(0) &= 0. \end{aligned}$$

The additive characters are defined as

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

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 also considered as an n -dimensional linear vector space and there is a basis $\{\sigma_j, j = 1, \dots, n\}$ in this vector space, so that any

$$\alpha \in GF(p^n), \quad \alpha = \sum_{j=1}^n a_j \sigma_j, \quad a_j \in \mathbb{Z}_p.$$

Then, for any $f(\alpha)$ one have

$$\sum_{\alpha \in GF(p^n)} f(\alpha) = \sum_{a_1, \dots, a_n} f(a_1 \sigma_1 + \dots + a_n \sigma_n). \quad (3)$$

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

Two bases $\{\alpha_1, \dots, \alpha_n\}$ and $\{\beta_1, \dots, \beta_n\}$ in the same field are dual if $\text{tr}(\alpha_i \beta_j) = \delta_{ij}$.

A basis which is dual to itself is called *self-dual basis*, $\text{tr}(\alpha_i \alpha_j) = \delta_{ij}$.

In the case of $GF(2^2)$ the elements $\{\theta, \theta^2\}$ are roots of the primitive polynomial. The polynomial basis is $\{1, \theta\}$, whose dual basis is $\{\theta^2, 1\}$:

$$\begin{aligned} \text{tr}(1\theta^2) &= 1, & \text{tr}(11) &= 0, \\ \text{tr}(\theta\theta^2) &= 0, & \text{tr}(\theta 1) &= 1. \end{aligned}$$

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

$$\begin{aligned} \text{tr}(\theta\theta) &= 1, & \text{tr}(\theta\theta^2) &= 0, \\ \text{tr}(\theta^2\theta) &= 0, & \text{tr}(\theta^2\theta^2) &= 1. \end{aligned}$$

The self-dual basis can not always be found and the following important Theorem takes place:

Theorem. For every prime power $d = p^n$, there exists an almost self-dual basis of $GF(p^n)$ over \mathbb{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: $\text{tr}(\theta_i \theta_j) = 0$ when $i \neq j$ and $\text{tr}(\theta_i^2) = 1$, with one possible exception. For instance, in the case of $GF(3^2)$ a self-dual basis does not exist and two elements $\{\theta^2, \theta^4\}$, θ being a root of the irreducible polynomial $x^2 + x + 2 = 0$, form an almost self-dual basis, i.e.

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

In the case of power of prime dimensions instead of natural numbers we have to use elements of the finite field $GF(d)$ to label states of the system and operators acting on the corresponding Hilbert space. In particular, we will denote as

$$|\alpha\rangle, \quad \alpha \in GF(d), \quad \langle\alpha|\beta\rangle = \delta_{\alpha,\beta}.$$

an orthonormal basis in the Hilbert space of the quantum system.

Operationally, the elements of the basis can be labelled by powers of primitive elements. These vectors will be considered as eigenvectors of the generalized position operator which belong to the generalized Pauli group, which generators are

$$Z_\beta |\alpha\rangle = \chi(\alpha\beta) |\alpha\rangle, \quad X_\beta |\alpha\rangle = |\alpha + \beta\rangle, \quad \alpha, \beta \in GF(d), \quad (4)$$

$$Z_\beta^\dagger = Z_{-\beta}, \quad X_\beta^\dagger = X_{-\beta}, \quad (5)$$

so that

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

where $\chi(\theta)$ is an additive character

$$\chi(\theta) = \exp \left[\frac{2\pi i}{p} \text{tr}(\theta) \right], \quad (6)$$

The characters (6) satisfy the following properties:

$$\sum_{\alpha \in GF(d)} \chi(\alpha\beta) = d\delta_{0,\beta}, \quad \chi(\alpha + \beta) = \chi(\alpha) \chi(\beta). \quad (7)$$

The operators (4) are related through the finite Fourier transform operator

$$F = \frac{1}{\sqrt{d}} \sum_{\alpha, \beta \in GF(d)} \chi(\alpha\beta) |\alpha\rangle \langle \beta|, \quad FF^\dagger = F^\dagger F = I, \quad (8)$$

so that

$$FX_\alpha F^\dagger = Z_\alpha, \quad (9)$$

and $F^4 = I$ for $d = p^n$ where $p \neq 2$, and $F^2 = I$ for $d = 2^n$.

The *conjugate* basis, which is related to the basis $|\alpha\rangle$

$$|\tilde{\alpha}\rangle = F |\alpha\rangle, \quad Z_\beta |\tilde{\alpha}\rangle = |\widetilde{\alpha + \beta}\rangle, \quad X_\beta |\tilde{\alpha}\rangle = \chi^*(\alpha\beta) |\tilde{\alpha}\rangle, \quad (10)$$

the elements of the conjugate basis are eigenvectors of the X_β operators.

Application: n - partite system with p energy levels. Hilbert space

$$\mathcal{H}_d \Leftrightarrow \mathcal{H}_p \otimes \mathcal{H}_{p..} \otimes \mathcal{H}_p$$

are labelled by elements of the basis

$$\{\sigma_1, \dots, \sigma_n\} : \alpha = a_1\sigma_1 + \dots + a_n\sigma_n, \quad a_j \in \mathbb{Z}_p,$$

so that

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

the coefficients a_j play the role of quantum numbers of each particle.

Example: $GF(2^2)$ the state

$$(|0\rangle + |\sigma^3\rangle) / \sqrt{2} \Leftrightarrow (|00\rangle + |11\rangle) / \sqrt{2}$$

in the self-dual basis (σ, σ^2)

The operators Z_α are factorized into a product of single particle Z operators

$$\begin{aligned} Z_\alpha &= Z^{a_1} \otimes \dots \otimes Z^{a_n}, \\ X_{\beta\alpha} &= X^{b_1} \otimes \dots \otimes X^{b_n}, \end{aligned}$$

$$\begin{aligned} \alpha &= a_1 \sigma_1 + \dots + a_n \sigma_n \\ \beta &= b_1 \sigma_1 + \dots + b_n \sigma_n \end{aligned}$$

The displacement operators

$$D(\alpha, \beta) = \phi(\alpha, \beta) Z_\alpha X_\beta, \quad (11)$$

$$(12)$$

$$\phi(\alpha, \beta) \phi^*(\alpha, \beta) = 1 \quad (13)$$

Orthogonality

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

where Tr means the operational trace in the Hilbert space,

Phase condition $\text{char}(GF(d)) \neq 2$

$$\phi(\alpha, \beta) \phi(-\alpha, -\beta) = \chi(-\alpha\beta), \quad (14)$$

$\text{char}(GF(d)) = 2$,

$$\phi^2(\alpha, \beta) = \chi(\alpha\beta), \quad (15)$$

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

The discrete space $GF(d) \times GF(d)$: a set of points $(\alpha, \beta) \in GF(d) \times GF(d)$

Lines:

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

where ζ, η, ϑ are some fixed elements of $GF(d)$ is called a straight line.

Rays

$$\alpha = 0, \quad \text{or} \quad \beta = \mu\alpha \quad (16)$$

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

There are $d-1$ parallel lines to each of $d+1$ rays, so that the total number of lines is $d(d+1)$.

The displacement operators labelled with points of the phase space belonging to the same ray commute

$$Z_{\alpha_1} X_{\beta_1=\mu\alpha_1} Z_{\alpha_2} X_{\beta_2=\mu\alpha_2} = Z_{\alpha_2} X_{\beta_2=\mu\alpha_2} Z_{\alpha_1} X_{\beta_1=\mu\alpha_1},$$

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

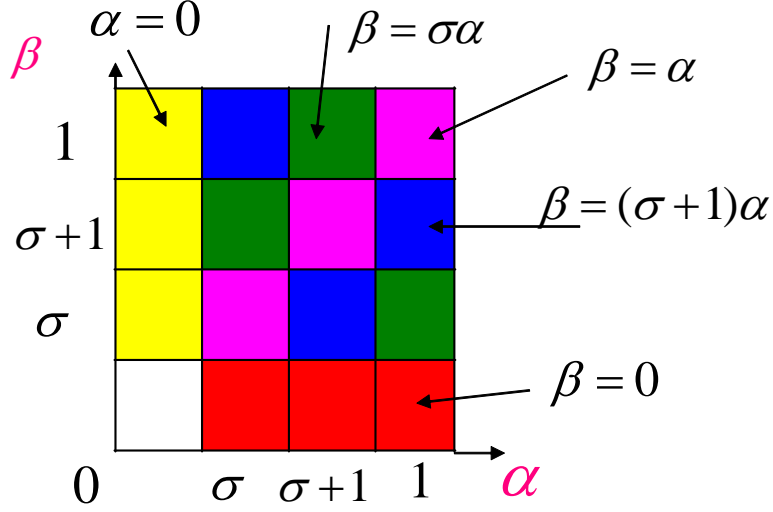


Figure 3:

$$Z_\alpha X_{\mu\alpha} |\psi_\nu^\mu\rangle = \chi(\alpha\nu) \exp(i\varphi(\alpha, \mu)) |\psi_\nu^\mu\rangle, \quad (17)$$

$$(18)$$

$$|\psi_\nu^\mu\rangle = X_\nu |\psi_0^\mu\rangle, \quad (19)$$

where μ is fixed

$|\tilde{\psi}_\nu^0\rangle = F |\psi_\nu^0\rangle \equiv |\tilde{\nu}\rangle$ are the eigenstates of the X_β operators (displacement operators labelled with the points of the ray $\alpha = 0$ - vertical axis).

The state $|\psi_\nu^\mu\rangle$ is associated with the line $\beta = \mu\alpha + \nu$.

The "rotation" operators $V_{\mu'}$ transform eigenstates of the operators associated with the ray $\beta = \mu\alpha$ into eigenstates of the operators corresponding to the ray $\beta = (\mu + \mu')\alpha$

$$V_\mu Z_\alpha V_\mu^\dagger = \exp(i\phi(\alpha, \mu)) Z_\alpha X_{\mu\alpha}, \quad [V_\mu, X_\nu] = 0, \quad V_0 = I,$$

where

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

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

$$\exp(i\varphi(\alpha, \mu)) = c_{\alpha, \mu} c_{0, \mu}^* = c_{\alpha, \mu}, \quad (20)$$

that is

$$c_{\kappa+\alpha, \mu} c_{\kappa, \mu}^* = c_{\alpha, \mu} \chi(-\mu\alpha\kappa), \quad (21)$$

and substituting $\alpha = 0$ we get $|c_{\kappa,\mu}|^2 = 1$

For fields of odd characteristics

$$c_{\kappa,\mu} = \chi(-2^{-1}\kappa^2\mu), \quad (22)$$

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 $V_\mu^\dagger = V_{-\mu}$.

V_μ transforms a state associated with the ray λ_μ into a state associated with the ray $\lambda_{\mu+\mu'}$.

$$V_\mu V_{\mu'} = V_{\mu+\mu'}, \quad (23)$$

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

$$\lambda_\mu \xrightarrow{V_{\mu'}} \lambda_{\mu+\mu'}, \quad (24)$$

For $\text{char}(GF(d)) = 2$ it follows from (21) that (substituting $\kappa = \alpha$)

$$c_{\alpha,\mu}^2 = \chi(\alpha^2\mu), \quad (25)$$

V_μ^2 is not the identity operator

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

Example: $GF(2^2)$

$$V_\theta = \text{diag}(1, 1, i, -i), \quad V_{\theta^2} = \text{diag}(1, i, 1, -i), \quad V_{\theta^3} = \text{diag}(1, i, i, -1), \quad (26)$$

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

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

MUB states $\{|\psi_\nu^\mu\rangle, \mu, \nu \in GF(d)\}$ associated to lines $\beta = \mu\alpha + \nu$

$$|\langle \psi_\nu^\mu | \psi_{\nu'}^{\mu'} \rangle|^2 = \frac{1}{d}, \quad \mu \neq \mu'.$$

Mapping kernels

$$\hat{w}^{(s)}(\alpha, \beta) = \frac{1}{d} \sum_{\kappa, \lambda \in GF(d)} \chi(\alpha\lambda - \beta\kappa) D(\kappa, \lambda) [\langle \xi | D(\kappa, \lambda) | \xi \rangle]^{-s}. \quad (27)$$

So that, in any self-dual basis for $\text{char}(GF(d)) \neq 2$

$$\hat{w}^{(s)}(\alpha, \beta) = \otimes \Pi_{i=1}^n \hat{w}^{(s)}(\alpha_i, \beta_i)$$

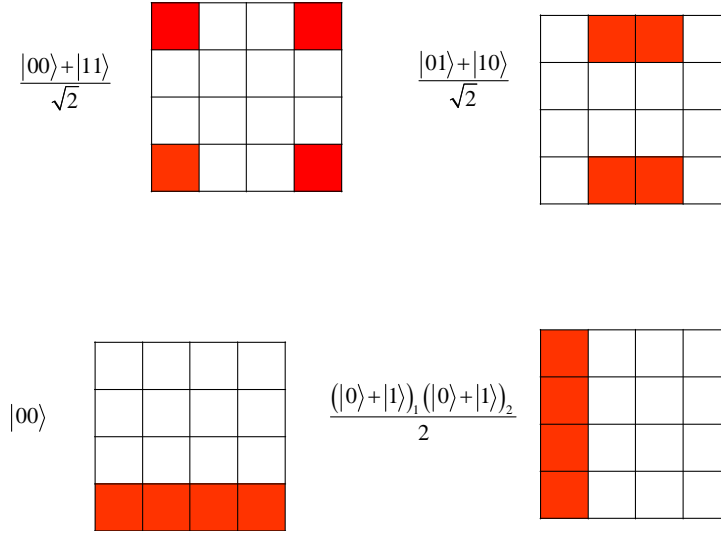


Figure 4:

The symbols of the operators Z_κ and X_λ are

$$W_{Z_\kappa}(\alpha, \beta) = \chi(\beta\kappa), \quad W_{X_\lambda}(\alpha, \beta) = \chi(-\alpha\lambda) \quad (28)$$

Symbols of the states

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

Tomographic condition

$$\frac{1}{d} \sum_{\alpha, \beta \in GF(d)} W(\alpha, \beta) \delta_{\beta, \mu\alpha + \nu} = \langle \psi_\nu^\mu | \rho | \psi_\nu^\mu \rangle, \quad (29)$$

Reconstruction relation

$$\rho = \sum_{\alpha, \beta} Tr(\rho \hat{\Pi}(\alpha, \beta)) \underbrace{\hat{\Pi}(\alpha, \beta)}_{\substack{\text{projectors to the states} \\ \text{corresponding to lines crossing } (\alpha, \beta)}} - \hat{I}$$

There are not only lines, but also "curves"

$$\beta = f_\mu(\alpha)$$

so that the commuting set of operators is

$$Z_\alpha X_{f_\mu(\alpha)}$$



Single qubit tomography

$$\text{z-basis: } \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}; \text{ x-basis: } \left\{ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}; \text{ y-basis: } \left\{ \frac{1}{\sqrt{2}} \begin{bmatrix} i \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} -i \\ 1 \end{bmatrix} \right\}$$

$$\text{Measurement in z-basis } \{|0\rangle, |1\rangle\} \Rightarrow \rho_{00}, \rho_{11}$$

$$\text{Measurement in x-basis, } \left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\} \Rightarrow \text{Re } \rho_{10}$$

$$\text{Measurement in y-basis, } \left\{ \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \right\} \Rightarrow \text{Im } \rho_{10}$$

$$\left. \begin{array}{l} \Rightarrow \text{Re } \rho_{10} \\ \Rightarrow \text{Im } \rho_{10} \end{array} \right\} \Rightarrow \begin{bmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{bmatrix}$$

$$\text{Relation between z, x and y bases: } |n\rangle_x = U_x |n\rangle_z, |n\rangle_y = U_y |n\rangle_z, n = 0, 1$$

local transformations

3 measurement sets

Figure 5:



Two qubit tomography:

Measurements in zz - basis $\Rightarrow \rho_{00,00}, \rho_{11,11}, \rho_{00,11}, \rho_{11,00}$

Measurements in locally rotated basis

$\underbrace{U_x^1 |n_1\rangle_z |n_2\rangle_z}_{xz} \Rightarrow \text{non-diagonal elements} + \text{diagonal elements}$

$${}_z\langle 00 | U_x^1 \rho U_x^1 | 00 \rangle_z = \rho_{00,00} + \rho_{01,00} + \rho_{10,00} + \rho_{11,00}$$

$\underbrace{U_y^1 |n_1, n_2\rangle_z}_{yz} \Rightarrow \text{non-diagonal elements} + \text{diagonal elements}$

$$\langle 00 | U_y^1 \rho U_y^1 | 00 \rangle = \rho_{00,00} - \rho_{11,11} + i\rho_{01,00} - i\rho_{10,00}$$

9 measurement sets + accumulations of errors

Figure 6:

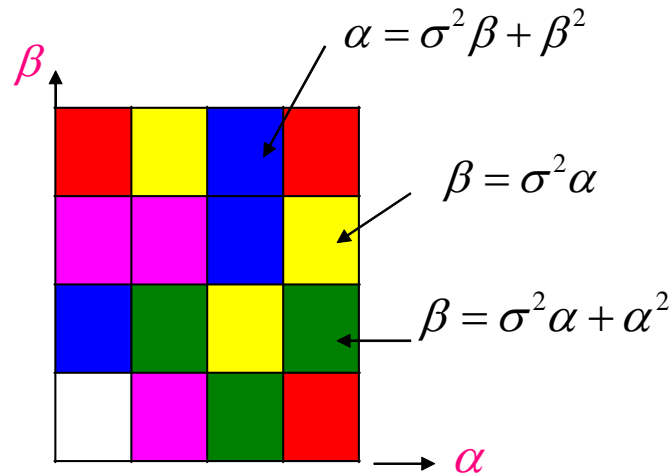


Figure 7:

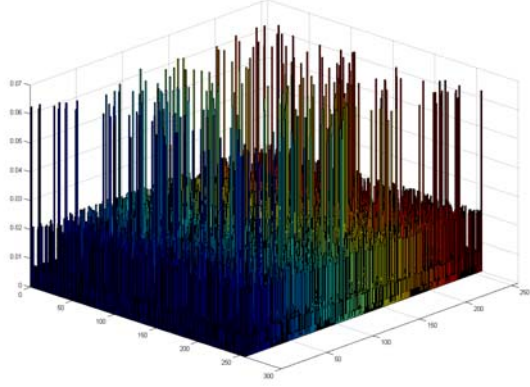


Figure 8:

Typical form of the Wigner function for N-qubit stateSpin coherent state

$$|\mathbf{n}\rangle_1|\mathbf{n}\rangle_2\ldots|\mathbf{n}\rangle_N$$

Correlation detection

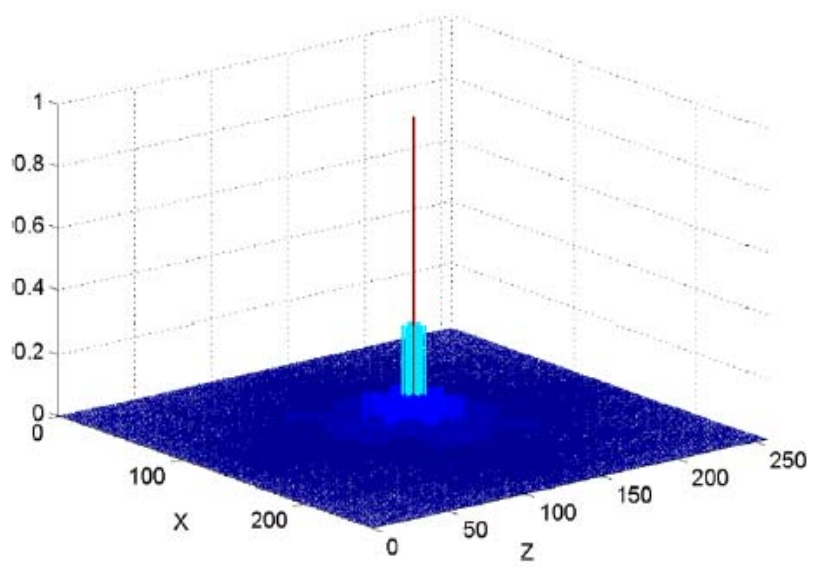
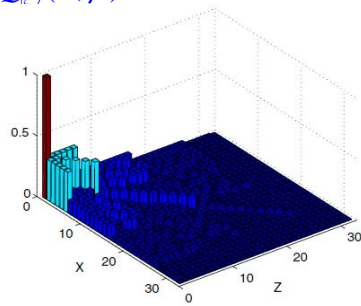


Figure 9:

Detecting quantum correlations

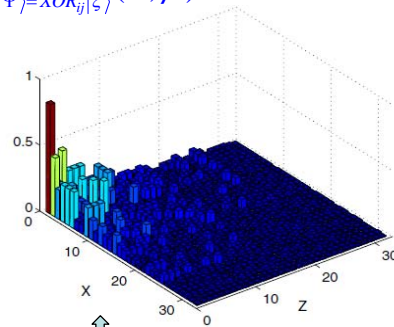
The Q -function for a factorized state $|\xi\rangle = |\mathbf{n}\rangle_1 \dots |\mathbf{n}\rangle_N$

$$Q_{|\xi\rangle}(\alpha, \beta)$$



Uncorrelated spins

$$Q_{|\Psi\rangle=XOR_{ij}|\xi\rangle}(\alpha, \beta)$$



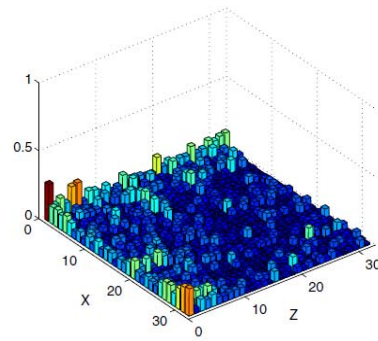
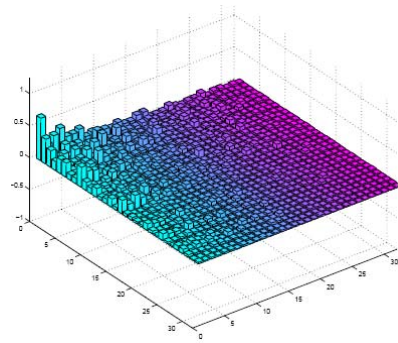
There are correlated particles

Figure 10:

Detecting quantum correlations

$$Q_{XOR_{kl} XOR_{ij}}(\alpha, \beta)$$

Q – function for highly correlated states



Measure of quantum fluctuations $\Upsilon = \sum_{\alpha, \beta} Q^2_{|\Psi\rangle}(\alpha, \beta) \leq \Upsilon_{|n_1\rangle_1 \dots |n_N\rangle_N}$

Figure 11: