Applications of the Heisenberg-Weyl group to Quantum State Tomography in infinite and finite dimensional Hilbert spaces (with a focus on dimensions 2 and 3).

Thomas Durt.

Ecole Centrale de Marseille

Institut Fresnel

thomas.durt@centrale-marseille.fr

Preamble: H-W group in $\mathcal{L}^2(\mathbb{R})$: definition.

The elements of the Heisenberg-Weyl group are obtained by composing

- “translations” in space (x): $e^{i\frac{\delta x\cdot\hat{p}}{\hbar}}$
- with “boosts” (translations in momentum space (p)): $e^{i\frac{\delta p\cdot\hat{x}}{\hbar}}$;
- In position representation (x), the generator of translations is $\hat{p} = \frac{\hbar}{i}\hat{\nabla}_x$ and $e^{i\frac{\delta x\cdot\hat{p}}{\hbar}}f(x) = e^{\delta x\cdot\frac{\partial}{\partial x}}f(x) = f(x+\delta x)$.
- In momentum representation (k) the generator of boosts is $\hat{x} = \frac{1}{i}\nabla_k$ and $e^{i\frac{\delta p\cdot\hat{x}}{\hbar}}g(k) = e^{(\delta p/\hbar)\cdot\frac{\partial}{\partial k}}g(k)$=$g(k+(\delta p/\hbar))$
- The H-W group is thus a representation of the Galilei group (translations in phase-space).

Preamble: H-W group in $\mathcal{L}^2(\mathbb{R})$: definition.

- Boosts and translations do not commute;
- Making use of the Baker-Campbell-Hausdorff formula
  $Z = X + Y + \frac{1}{2}[X, Y] + \frac{1}{12}([X, [X, Y]] - [Y, [X, Y]]) + ...$
  which is the solution for Z to the equation $e^X \cdot e^Y = e^Z$,
- it is straightforward to derive Weyl relations:
  $e^{i\frac{\delta x \cdot \hat{p}}{\hbar}} e^{i\frac{\delta p \cdot \hat{x}}{\hbar}} = e^{i\frac{\delta x \cdot \delta p}{\hbar}} e^{i\frac{\delta p \cdot \hat{x}}{\hbar}} e^{i\frac{\delta x \cdot \hat{p}}{\hbar}}$
- wikipedia: *...These relations may be thought of as an exponentiated version of the canonical commutation relations; they reflect that translations in position and translations in momentum do not commute...*
- Discrete representations of the H-W group are most often[a] very fidel to their counterpart in the continuum as we shall show.

[a]X. Lu, P. Raynal and B-G Englert, PHYSICAL REVIEW A 85, 052316 (2012), Mutually unbiased bases for the rotor degree of freedom.

Preamble: coherent states in $\mathcal{L}^2(\mathbb{R})$.

Displacement operators in $\mathcal{L}^2(\mathbb{R})$ possess numerous applications, e.g. coherent states of an harmonic oscillator are displaced vacuum states:

Two definitions of a coherent state $|\alpha>$

- Definition 1: a coherent state is an eigenstate of the lowering (annihilation) operator a, for a complex eigenvalue α.
- Definition 2: such a coherent state can also be defined as follows: $|\alpha>_{coherent}= exp^{\alpha a^\dagger - \alpha^* a}|E_0>= exp^{i\sqrt{2m\omega/\hbar}((-Re.\alpha)\cdot\hat{p}/m\omega+(Im.\alpha)\cdot\hat{x})}|E_0>$, where $|E_0>$ is the ground state of the harmonic oscillator.
- Indeed, making use of the Baker-Campbell-Hausdorff formula, $e^{\alpha a^\dagger}\cdot e^{-\alpha^* a} = e^{|\alpha|^2/2}e^{\alpha a^\dagger - \alpha^* a}$;
  therefore $e^{\alpha a^\dagger - \alpha^* a}|E_0>= e^{-|\alpha|^2/2}e^{\alpha a^\dagger}\cdot e^{-\alpha^* a}|E_0>$,
  but $e^{-\alpha^* a}|E_0>= |E_0>$ and $(a^\dagger)^N|E_0>= \sqrt{N!}|E_N>$ so that
  $e^{\alpha a^\dagger - \alpha^* a}|E_0 \quad >= \quad e^{-|\alpha|^2/2}e^{\alpha a^\dagger}|E_0 \quad >=e^{-|\alpha|^2/2}\sum_{N=0}^{\infty}\frac{\alpha^N\sqrt{N!}}{N!}|E_N \quad >=$ $|\alpha>_{coherent}$, establishing the equivalence of definitions 2 and 1.

Preamble. qubit case, displacements in dimension 2.

- The translation group contains two elements: the sigma X operator that translates the states of the computational basis, and its square, the identity operator (sometimes denoted sigma 0):
  $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- The qubit counterpart of the momentum representation consists of eigenstates of the displacement operator (as is the case in the continuum case).
- These are the states $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ and $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$
- The qubit boosts displace these eigenstates. They thus consist of two elements, the identity and the sigma X operator sandwiched in a Hadamard transform; this is the sigma Z operator $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- one can check that $\sigma_z \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$.

Preamble. qubit case, displacements in dimension 2.

- Finally composing the translations and the boost generators we get sigma Y (up to a global phase).

$$i\sigma_y = i \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

- The discrete counterpart of the Heisenberg-Weyl group in dimension 2 (qubits) is the Pauli group.

Preamble. qubit case,

displacements in dimension 2 and Bell states.

As is well-known, (two qubit) Bell states are defined as follows
$|B^0_0\rangle = \frac{1}{\sqrt{2}}(|+\rangle^A_Z \otimes |+\rangle^B_Z + |-\rangle^A_Z \otimes |-\rangle^B_Z)$
$|B^0_1\rangle = \frac{1}{\sqrt{2}}(|-\rangle^A_Z \otimes |+\rangle^B_Z + |+\rangle^A_Z \otimes |-\rangle^B_Z)$
$|B^1_0\rangle = \frac{1}{\sqrt{2}}(|+\rangle^A_Z \otimes |+\rangle^B_Z - |-\rangle^A_Z \otimes |-\rangle^B_Z)$
$|B^1_1\rangle = \frac{1}{\sqrt{2}}(|+\rangle^A_Z \otimes |-\rangle^B_Z - |-\rangle^A_Z \otimes |+\rangle^B_Z)$.
They are in one to one correspondence with the Pauli operators (to pass from Pauli operators to Bell states it suffices to formally replace $|...\rangle\langle'''|$ by $|...\rangle^A_Z \otimes |'''\rangle^B_Z$.
The trick also holds in dimension d, where (two qu$d$it) Bell states obey, in the most simple cases, the following definition:

$$|B_{m,n}\rangle = d^{-1/2}\sum_{k=0}^{d-1}\gamma^{(k.n)}|k\rangle \otimes |k+m(modulod)\rangle \tag{1}$$

(where $\gamma = e^{\frac{i2\pi}{d}}$). In dimension $d=2$ we recover the Bell states defined above.

Preamble. qubit case,

displacements in dimension 2 and Bell states.

In dimension d Bell states obey the following identity (cfr exercices):

$$V_{m,A}^{n} \otimes 1_B |B_{0,0}\rangle_{A,B} = |B_{m,n}\rangle_{A,B} \tag{2}$$

where the discrete (qu$d$it) displacement operators are defined as follows

$$V_i^j = \sum_{k=0}^{d-1} \gamma^{((k+i)\cdot j)} |k+i\rangle\langle k|; i, j : 0...d-1 \tag{3}$$

In particular, when $d = 2$, these displacement operators are (up to global phase) the Pauli operators (cfr exercices):

$$V_0^0 = \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, V_1^0 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$V_1^1 = i\sigma_y = i\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \text{while } \mathrm{V}_0^1 = \sigma_\mathrm{z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Applications of the Pauli group to Quantum Information:

- Quantum information cannot be cloned but it can be teleported, densely coded and entanglement can be swapped as we shall now show. The displacement group plays a prior role in these applications.
- Potential applications concern relays for QKD, based on entanglement swapping and teleportation.
- Such relays would allow to refresh keys on long distances, getting rid of the limitations imposed by the absoption in optical fibres (50 percent every 50 kilometer-joined with the dark count rate in detectors).
- To the contrary of QKD, teleportation and entanglement swapping did not mature enough to reach the level of a commercialisable technology, but presently several research groups devote a lot of energy to quantum memories, a crucial challenge to be met along the road of massive production of entanglement-based relays...
- Before focusing on tomographic applications of the displacement group, we shall give a quick overlook of teleportation, dense coding and entanglement swapping.

Qubit teleportation: theory.

- The "equation" of teleportation is:

$$(\sum_{i=0}^{1}\phi_i|i\rangle_A)|B_{0,0}\rangle_{B,C} = \sum_{m,n=0}^{1}\frac{1}{2}|B_{m,n}\rangle_{A,B}(\sigma_{m,n}(\sum_{i=0}^{d-1}\phi_i|i\rangle_C)), \qquad (4)$$

where the $\sigma_{m,n}$ represent the conveniently labelled Pauli operators.
Other expression (see exercises for the proof):

$$(\phi_0|0\rangle_A + \phi_1|1\rangle_A)(\frac{1}{\sqrt{2}}(|0\rangle_B|0\rangle_C + |1\rangle_B|1\rangle_C))$$

$$= \frac{1}{2}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)\frac{1}{\sqrt{2}}(\phi_0|0\rangle_C + \phi_1|1\rangle_C)$$

$$+ \frac{1}{2}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)\frac{1}{\sqrt{2}}(\phi_0|0\rangle_C - \phi_1|1\rangle_C)$$

$$+ \frac{1}{2}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)\frac{1}{\sqrt{2}}(\phi_0|1\rangle_C + \phi_1|0\rangle_C)$$

$$+ \frac{1}{2}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)\frac{1}{\sqrt{2}}(\phi_0|1\rangle_C - \phi_1|0\rangle_C)$$

Qubit teleportation: in practice.

- Bob and Charles share the two-qubit Bell state $|B_0^0\rangle$.
- Alice sends a qubit prepared in an arbitrary state $\phi_0|0\rangle_A + \phi_1|1\rangle_A$ to Bob.
- Bob measures the pair in the Bell basis.
- By doing so he projects, whenever he gets the result m, n (m and n vary from 0 to 1) Charles's state onto $\sigma_{m,n}(\phi_0|0\rangle_C + \phi_1|1\rangle_C)$.
- Bob uses a classical communication line to inform Charles about which result he got.
- Charles applies onto his photon the operator $\sigma_{m,n}$; as the square of Pauli operators is equal to unity, he recovers the state $(\phi_0|0\rangle_C + \phi_1|1\rangle_C)$, which is a teleported version of Alice's original state.

Warning: difference between Star Trek teleportation and Quantum Teleportation.

- No matter is teleported during quantum teleportation (Charles's qubit was already present).
- In accordance with the no signaling theorem (APPENDIX), no classical information is teleported: Charles has to wait until he receives Bob's message before he can reproduce Alice's state. Otherwise, his qubit is in a fully noisy state (no ”in”formation implies no form!).
- Nevertheless, a continuous variable (the location of a point on the Bloch sphere) gets teleported and this requires only a classical communication of two classical bits (m, n).

Remark:

During a teleportation process, the copy is created at Charles's level while the original qubit that was prepared by Alice gets simultaneously destroyed: teleportation is a ”no cloning process”.

Quantum Dense Coding.
After preparing the Bell state $|B_{0,0}\rangle_{A,B}$, one can generate the three other Bell states by applying onto one of the qubits the Pauli operators.
This is a particular case of the aforementioned identity

$$V^n_{m,A} \otimes 1_B |B_{0,0}\rangle_{A,B} = |B_{m,n}\rangle_{A,B} \tag{5}$$

where the discrete (qu$d$it) displacement operators are defined as follows

$$V_i^j = \sum_{k=0}^{d-1} \gamma^{((k+i)\cdot j)} |k+i\rangle\langle k|; i, j : 0...d-1 \tag{6}$$

In particular, when $d = 2$, these displacement operators are (up to global phase) the Pauli operators.

Quantum Dense Coding.
In the practice, the identity $V^n_{m,A} \otimes 1_B |B_{0,0}\rangle_{A,B} = |B_{m,n}\rangle_{A,B}$ can be implemented as follows:
Alice, by acting merely on the qubit in her possession, can transform the Bell state $|B_{0,0}\rangle_{A,B}$ in one of the four Bell states.
Those states form an orthonormal basis which makes it possible to realize a protocol of "dense coding" defined as follows:

- Alice and Bob share a Bell state ($|B_{0,0}\rangle_{A,B}$).
- Alice applies to the qubit in her possession one of the four Pauli operators, chosen at random, (these are the identity operator σ_0, σ_X, σ_Y, and σ_Z).
- Afterwards, she sents to Bob her qubit and Bob measures the two qubits (the one sent by Alice and the one in his possession since the beginning) in the Bell basis.
- By doing so, Bob gets informed about the choice made by Alice in her choice of the Pauli operator.

Finally:
Alice sent one qubit, but two classical bits of information (this is impossible with a classical support for the information: one classical bit cannot be compressed). This is the essence of DENSE CODING.
All this generalizes to the case of qu$d$its (dimension d): then, by sending one physical, quantum $d$it, a qu$d$it, Alice is able to send two classical $d$its.

Entanglement swapping. Theory

Swapping means permutation.

- The "equation" (basic identity of) of qubit entanglement swapping is:

$$|B_{0,0}\rangle_{A,B}|B_{0,0}\rangle_{C,D} = \frac{1}{4}\sum_{i,j=0}^{1}|B_{i,j}\rangle_{B,C}|B_{i,j}\rangle_{A,D} = \sum_{i,j=0}^{1}|B_{i,j}\rangle_{B,C}\sigma_{i,j}|B_{0,0}\rangle_{A,D},$$

where the $\sigma_{m,n}$symbols represent the Pauli operators and where we made use of the basic identity of dense coding $V_{m,A}^{n}\otimes 1_B|B_{0,0}\rangle_{A,B} = |B_{m,n}\rangle_{A,B}$, in the qubit case (where $V_m^n = \sigma_{m,n}$).

The demonstration of a similar basic identity of qu$d$it entanglement swapping is left as an exercise.

Entanglement swapping: In practice.

- Alice and Bob share the-entangled-Bell state $|B_0^0\rangle^{AB}$. Charles and Daisy share the-entangled-Bell state $|B_0^0\rangle^{CD}$.

  Alice and Daisy can be located in principle in arbitrary distant regions but Bob and Charles are supposed to meet each other, in order to put their bits in common for measuring them in the-entangled-Bell basis

- If by doing so they measure the result m, n (m and n can take two values: 0 and 1, and each result has probability one fourth), then Alice and Daisy qubits get projected onto the state $|B_n^m\rangle^{AD} = \sigma_{m,n}^A |B_0^0\rangle^{AD}$.

- Bob and Charles warn Alice and Daisy, on a public channel (slower than light of course) about their result (one result among four possible results).

- Alice lets act onto her qubit the operator $\sigma_{m,n}$, in the case that Bob and Charles obtained the result (m, n); by doing so she transforms the state of the pair of qubits that she shares with Daisy into the bell state $|B_0^0\rangle^{AD}$.

- Conclusion, the entanglement that Alice shared with Bob and Daisy with Charles has been swapped; at this level Alice and Daisy share a maximally entangled state, although possibly they were never in contact in the past...

- Morality: my friends's friends's friends are also my friends.

Remark.

As mentioned before, relays based on entanglement swapping and teleportation would make it possible to increase arbitrarily the distance of QKD. It is indeed impossible to amplify a quantum signal due to the no-cloning theorem although nothing forbids to teleport it...

Quantum displacements:tomographic applications.

- In the rest of this talk we shall focus on tomographic applications.
- Quantum state tomography in finite dimension d aims at estimating the $d^2 - 1$ real parameters necessary for characterizing the density operator representing the state of a qu$d$it.
- We shall firstly describe some geometric properties of phase-space representations, like Weyl and Wigner representations, in the continuum ($\mathcal{L}^2(\mathbb{R})$).
- We shall then describe related tomographic protocols involving the (discrete version of the) Heisenberg-Weyl group, which consists of d^2 displacements in a discrete d times d phase-space associated to the qu$d$it.

Quantum displacements:tomographic applications.

- Some of these protocols are directly related to their counterpart in infinite dimension, like Weyl and Wigner tomography.
- New structures appear throughout this study: mutually unbiased bases (MUBs) and symmetric informationally complete POVMs (SICs).
- In dimensions 2 and 3, MUBs, SICs, Wigner and Weyl tomography are intimately connected to each other as we shall see...

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- Displacement operators are orthonormal relatively to the Trace product; therefore a linear operator $\hat{O}$ can be expressed as a superposition of displacement operators through Groenewold's formula[a]
$\hat{O} = (1/h) \int \int dpdq e^{ip\hat{x}/\hbar + ix\hat{p}/\hbar} Tr(e^{(-ip\hat{x}-ix\hat{p})/\hbar}\hat{O})$
- In particular, when $\hat{O}$ is a density operator $\hat{\rho}$, the expression $Tr(e^{(-ip\hat{x}-iq\hat{p})/\hbar}\hat{\rho})$ delivers a tomographic representation of $\hat{\rho}$.
- This complex distribution changes by a phase factor under Galilean transformations:
$e^{-(i\delta p\hat{x}+i\delta q\hat{p})/\hbar} e^{(-ip\hat{x}-ix\hat{p})/\hbar} e^{(i\delta p\hat{x}+i\delta x\hat{p})/\hbar} = e^{i((x\delta p - p\delta x)/\hbar)} \cdot e^{(-ip\hat{x}-ix\hat{p})/\hbar}$.
- It is worth noting that this phase is related to the symplectic scalar product:
$x\delta p - p\delta x = (x, p) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \delta x \\ \delta p \end{pmatrix}$

[a] Curtright, T. L.; Fairlie, D. B.; Zachos, C. K. (2014). A Concise Treatise on Quantum Mechanics in Phase Space. World Scientific.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- The Wigner distribution delivers an alternative representation of $\hat{\rho}$.
- It is defined as $w(x,p) = (2/h) \int dy e^{-2ipy/\hbar} < x+y|\hat{\rho}|x-y >$.
- Making use of $e^{ix\hat{p}/\hbar}|y >= |y+x >$ and $< y|e^{ix\hat{p}/\hbar} =< y-x|$, of Weyl relations ($e^{i\frac{\delta x \cdot \hat{p}}{\hbar}} e^{i\frac{\delta p \cdot \hat{x}}{\hbar}} = e^{i\frac{\delta x \cdot \delta p}{\hbar}} e^{i\frac{\delta p \cdot \hat{x}}{\hbar}} e^{i\frac{\delta x \cdot \hat{p}}{\hbar}}$), and of the fact that the parity operator anticommutes with $\hat{x}$ and $\hat{p}$, it is easy to show that

  $w(x,p) = (2/h)Tr.(e^{ixp/\hbar} e^{2(ip\hat{x}/\hbar)} e^{(2ix\hat{p}/\hbar)} \cdot P\hat{a}r. \cdot \hat{\rho})$

  $= (2/h)Tr.(e^{2(ip\hat{x}/\hbar + ix\hat{p}/\hbar)} \cdot P\hat{a}r. \cdot \hat{\rho})$

  $= (2/h)Tr.(P\hat{a}r. \cdot e^{-2(ip\hat{x}/\hbar + ix\hat{p}/\hbar)} \cdot \hat{\rho})$

  $= (2/h)Tr.(e^{(ip\hat{x}/\hbar + ix\hat{p}/\hbar)} \cdot P\hat{a}r. \cdot e^{-(ip\hat{x}/\hbar + ix\hat{p}/\hbar)} \cdot \hat{\rho})$,

  where $P\hat{a}r.$ represents the parity operator: $P\hat{a}r.|y >= |-y >$.
- This means that the Wigner distribution is proportional to the trace of the product of $\hat{\rho}$ with the displaced parity operator: $w(x,p) = (2/h)Tr.\hat{W}(x,p) \cdot \hat{\rho}$

  where the Wigner operator obeys

  $\hat{W}(x,p) = e^{(ip\hat{x}/\hbar + ix\hat{p}/\hbar)} \cdot P\hat{a}r. \cdot e^{-(ip\hat{x}/\hbar + ix\hat{p}/\hbar)}$.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

Some remarks: Weyl distribution

- Let us introduce the displacement operators from now on denoted $\hat{U}_{x,p}$ and called the Weyl operators defined as follows
  $\hat{U}_{x,p} = e^{ixp/2\hbar} e^{ip\hat{x}/\hbar} e^{ix\hat{p}/\hbar} = e^{i(p\hat{x}/\hbar + x\hat{p})/\hbar}$.
  $\hat{U}_{x,p}$ is a unitary operator; it is not self-adjoint however. It is easy to show, e.g. with the help of Weyl relations ($e^{i\frac{\delta x \cdot \hat{p}}{\hbar}} e^{i\frac{\delta p \cdot \hat{x}}{\hbar}} = e^{i\frac{\delta x \cdot \delta p}{\hbar}} e^{i\frac{\delta p \cdot \hat{x}}{\hbar}} e^{i\frac{\delta x \cdot \hat{p}}{\hbar}}$), that if (x_1, p_1) is parallel to (x_2, p_2), then
  $\hat{U}_{x_1,p_1} . \hat{U}_{x_2,p_2} = \hat{U}_{x_1+x_2,p_1+p_2}$
- Both the Wigner and Weyl operators form a basis of the set of operators, orthonormal relatively to the Trace-scalar product
  $< \hat{O}_1, \hat{O}_2 >= Tr.(\hat{O}_1^\dagger \hat{O}_2)$
- From now on we shall call the Weyl distribution of ρ (denoted $u_{m,n}$) the (set of all) amplitudes of the expansion of ρ in the $U_{m,n}$ basis: $u_{m,n} = Tr.(\hat{U}_{m,n}\hat{O})$

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

Some remarks: Weyl versus Wigner distribution.

- As we have seen, the Wigner distribution is proportional to the trace of the product of $\hat{\rho}$ with the displaced parity operator: $w(x,p) = (2/h)Tr.\hat{W}(x,p)\cdot\hat{\rho}$

  where the Wigner operator obeys

  $\hat{W}(x,p) = e^{(ip\hat{x}/\hbar+ix\hat{p}/\hbar)}\cdot \hat{Par.}\cdot e^{-(ip\hat{x}/\hbar+ix\hat{p}/\hbar)}$.

- Moreover, $Tr.(e^{-i(a\hat{p}+b\hat{x})}\hat{Par.})$=$e^{-iab/2}\int dy < y|e^{-ia\hat{p}}e^{iby}|-y >$

  =$e^{-iab/2}\int dy < y-a|e^{iby}|-y >$

  =$e^{-iab/2}\int dy e^{iby}\delta(2y-a)$

  =$(1/2)e^{-iab/2}e^{iab/2}$ so that $\hat{Par.} = \frac{1}{2h}\int dxdp\hat{U}_{x,p}$.

  The parity operator appears thus to be a superposition with equal amplitudes of all displacement operators $U_{x,p}$.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

Some remarks: Weyl versus Wigner distribution.

- Finally, **the Wigner distribution appears to be, in this perspective, the symplectic transform of the Weyl distribution:**

$w(x,p) = (2/h)Tr.\hat{U}_{2x,2p}P\hat{a}r.O$=$(2/h)Tr.U_{2x,2p}\frac{1}{2h}\int dx'dp'\hat{U}_{x',p'}O$

=$\frac{1}{h^2}\int dx''dp''e^{i\frac{(x,p)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} x'' \\ p'' \end{pmatrix}}{\hbar}}(Tr.\hat{U}_{x'',p''}O)$, where the symplectic product of $\begin{pmatrix} x \\ p \end{pmatrix}$ and $\begin{pmatrix} x'' \\ p'' \end{pmatrix}$ is equal to $x \cdot p'' - p \cdot x''$.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

The Wigner distribution enjoys appealing properties:

- 1. the Wigner distribution of any self-adjoint operator ($\hat{\rho}$ in particular) is real valued (but not positive-definite, henceforth it is often called a quasi-distribution).
- 2. it transforms "naturally" under Galilean transformations.
- 3. its marginals have the same properties as in the case of a classical, positive-definite probability distribution over phase-space.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

1. the Wigner distribution of a self-adjoint operator is real valued.
PROOF:

- If $w(x,p) = (2/h)Tr.(e^{ixp/\hbar}e^{(2ip\hat{x}/\hbar)}e^{(2ix\hat{p}/\hbar)} \cdot P\hat{a}r. \cdot O)$ and $O = O^\dagger$,

  then $w^*(x,p) = (2/h)Tr.(O^\dagger \cdot P\hat{a}r.^\dagger \cdot (e^{ixp/\hbar}e^{(2ip\hat{x}/\hbar)}e^{(2ix\hat{p}/\hbar)})^\dagger)$
  $= (2/h)Tr.(O \cdot P\hat{a}r. \cdot (e^{-ixp/\hbar}e^{-2(ix\hat{p}/\hbar)}e^{-2(ip\hat{x}/\hbar)})$
  $= (2/h)Tr.(O \cdot (e^{-ixp/\hbar}e^{2ixp/\hbar}e^{(2ip\hat{x}/\hbar)}e^{(2ix\hat{p}/\hbar)}) \cdot P\hat{a}r.)$
  $= (2/h)Tr.(e^{2(ip\hat{x}/\hbar+ix\hat{p}/\hbar)} \cdot P\hat{a}r. \cdot O) = w(x,p)$

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

2. it transforms “naturally” under Galilean transformations.
PROOF:

- If $w(x,p) = (2/h)Tr.(e^{ixp/\hbar}e^{2(ip\hat{x}/\hbar)}e^{2(ix\hat{p}/\hbar)} \cdot \hat{Par.} \cdot \rho)$ and $\rho' = U_{\delta x,\delta p}\rho U^{\dagger}_{\delta x,\delta p}$,

  then, $w'(x,p) = (2/h)Tr.(e^{ixp/\hbar}e^{2(ip\hat{x}/\hbar)}e^{2(ix\hat{p}/\hbar)} \cdot \hat{Par.} \cdot \rho')$
  $= (2/h)Tr.(e^{ixp/\hbar}e^{2(ip\hat{x}/\hbar)}e^{2(ix\hat{p}/\hbar)} \cdot \hat{Par.} \cdot U_{\delta x,\delta p}\rho U^{\dagger}_{\delta x,\delta p})$
  $= (2/h)Tr.(U^{\dagger}_{\delta x,\delta p}e^{ixp/\hbar}e^{2(ip\hat{x}/\hbar)}e^{2(ix\hat{p}/\hbar)} \cdot \hat{Par.} \cdot U_{\delta x,\delta p}\rho)$

  Now, $U_{\delta x,\delta p} = e^{i\delta x\delta p/2\hbar}e^{i(\delta p\hat{x}/\hbar}e^{i\delta x\hat{p}/\hbar}$ and $U^{\dagger}_{\delta x,\delta p} = e^{-i\delta x\delta p/2\hbar}e^{-i\delta x\hat{p}/\hbar}e^{-i\delta p\hat{x}/\hbar}$

  thus $w'(x,p) =$
  $(2/h)Tr.(e^{-i\delta x\hat{p}/\hbar}e^{-i\delta p\hat{x}/\hbar}e^{ixp/\hbar}e^{2ip\hat{x}/\hbar}e^{2ix\hat{p}/\hbar} \cdot e^{-i\delta p\hat{x}/\hbar}e^{-i\delta x\hat{p}/\hbar} \cdot \hat{Par.}\rho)$
  $= (2/h)Tr.(e^{i(x-\delta x)(p-\delta p)/\hbar}e^{2(i(p-\delta p)\hat{x}/\hbar)}e^{2i(x-\delta x)\hat{p}/\hbar)} \cdot \hat{Par.} \cdot \rho)$
  $= (2/h)Tr.(e^{2(i(p-\delta p)\hat{x}/\hbar+i(x-\delta x)\hat{p}/\hbar)} \cdot \hat{Par.} \cdot \rho)$
  $= w(x-\delta x, p-\delta p)$

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

3. its marginals have the same properties as in the case of a classical, positive-definite probability distribution over phase-space.
PROOF:

- $\int dpw(x,p) = \int dp(2/h) \int dye^{-2ipy/\hbar} < x+y|\hat{\rho}|x-y >$
  $=(1/h)\hbar \int dy \int d(2p/\hbar)e^{-2ipy/\hbar} < x+y|\hat{\rho}|x-y >$
  $=(1/h)2\pi\hbar \int dy\delta^{Dirac}(y) < x+y|\hat{\rho}|x-y > = < x|\rho|x >$
- Reexpressing the density operator in the momentum representation, and making use of the properties of Fourier transforms, one can show by direct computation that the Wigner distribution
  $w(x,p) = (2/h) \int dye^{-2ipy/\hbar} < x+y|\hat{\rho}|x-y >$
  possesses a nearly similar expression in both representations:
  $w(x,p) = (2/h) \int dre^{+2irx/\hbar} < p \tilde{+} r|\hat{\rho}|p \tilde{-} r >$ where $|\tilde{p} >$ is a plane wave in the position representation, of wave number $k = p/\hbar$.
  so that by the same computation as above we get
  $\int dxw(x,p) = < p|\hat{\rho}|p >$.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

3. its marginals have the same properties as in the case of a classical, positive-definite probability distribution over phase-space.
PROOF (continued):

- In order to compute $\int dx w(x,p)$, an alternative approach consists of exploiting the Fourier duality between position and momentum and the properties of symplectic transforms.

- To see this, let us consider the action of $\hat{x}$ and $\hat{p}$ in momentum representation. To make things simpler let us introduce dimensionless variables q and k:

  q=$x/x_{car.}$, where $x_{car.}$ is a characteristic length;
  $\hat{k} = (1/i)\frac{\partial}{\partial q} = (1/i)\hat{\nabla}_q$, and $\Psi^F(k) =< k|\Psi >$=$\frac{1}{\sqrt{2\pi}} \int dq \Psi(q) e^{-ik\cdot q}$
  After integrating by parts we find that
  $(1/\sqrt{2\pi}) \int dk e^{ikq} (1/i)\nabla_k \Psi^F(k) = -q \cdot (1/\sqrt{2\pi}) \int dk e^{ikq} \Psi^F(k)$,
  while $(1/\sqrt{2\pi}) \int dk k \cdot e^{ikq} \Psi^F(k) = (1/i)\nabla_q (1/\sqrt{2\pi}) \int dk e^{ikq} \Psi^F(k)$
  so that passing from momentum to position representation $(1/i)\nabla_k$ corresponds to minus the multiplicative operator q while the multiplicative operator k corresponds to the operator $(1/i)\nabla_q$.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- In the same vein one can show that $\tilde{U}_{m,n}$ corresponds to $U_{-n,m}$ where the tilded operator refers to momentum representation and the non-tilded operator to the position representation. It is worth noting that the mapping between (m,n) and (m',n') preserves the symplectic product:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^T \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

- Now, the Wigner distribution is as already shown, the symplectic transform of the Weyl distribution: $w(x,p)$

$$=(2/h) Tr.U_{2x,2p} P\hat{a}r.O = \frac{1}{h^2} \int dx'' dp'' e^{i \frac{(x,p) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x'' \\ p'' \end{pmatrix}}{\hbar}} (Tr.U_{x'',p''} O)$$

- Conclusion: $\tilde{w}_{m',n'} = w_{m,n}$ where $\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- The marginals obtained after integrating along vertical lines in the momentum representation are thus equal to the marginals obtained after integrating along horizontal lines in the position representation. The transformation $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ permutes these two directions. We find thus that the marginals obtained after integrating over x (p) are the probabilities to find p (x).
- **What is less known[a] is that the marginal property generalizes in this way to arbitrary directions in the phase-space.**
- **It can be shown by lengthy but elementary computations that these directions are related to the vertical direction by a symplectic transformation parameterized by a real parameter α as follows:** $\begin{pmatrix} 0 & 1 \\ -1 & -\alpha \end{pmatrix}$
- It is worth noting that the mapping between (m, n) and (m', n') preserves the symplectic product:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -\alpha \end{pmatrix}^T \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -\alpha \end{pmatrix}$$

[a] W. K. Wootters, Ann. Phys. (N.Y.) 176 1 (1987), A Wigner function formalism of finite-state quantum mechanics.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- When $\alpha = 0$ it sends the position representation onto a complementary representation which coincides with the momentum representation.
- In the new basis the displacement operators are the same as in the position basis but they are permuted:
  $U_{n',-\alpha n'-m}$=$\tilde{U}^{\alpha}_{m',n'}$
- In particular $U_{m,-\alpha m}$=$\tilde{U}^{\alpha}_{0,m}$.
- It maps the vertical lines parallel to $(m = 0, n = 1)$ onto parallel lines of slope $-\alpha$. Accordingly, marginals along this direction deliver probabilities associated to the generalized Fourier states $|\tilde{k}_\alpha >$ which diagonalize the displacement operators $U_{m,-\alpha m}$.
- The inverse mapping also preserves the symplectic product.
- All these properties are well-known and are related to the Clifford group[a].
- Similarly, the Wigner operators are also permuted one by one under this change of representation: $W_{m,n}$ = $\tilde{W}^{\alpha}_{-\alpha m-n,m}$ (where again the tilded operator with an upper index α refers to the generalised momentum representation and the non-tilded operator to the position representation).

[a] M. Appleby, I. Begtsson and M. Chaturvedy, Journal of Mathematical Physics 49, 012102 (2008), Spectra of phase point operators in odd prime dimensions and the extended Clifford group.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- *Definition: "A collection of orthonormal bases of a* d *dimensional Hilbert space is said to be mutually unbiased if whenever we choose two states from different bases, the modulus squared of their in-product is equal to* $1/d$*. "*
- Here there appears an infinity of bases constituted by the generalized Fourier states $|\tilde{k}_\alpha>$ which diagonalize the displacement operators $U_{m,-\alpha m}$.
- $< x|\tilde{k}_\alpha >= \frac{1}{\sqrt{2\pi}} e^{i(k\cdot q+\alpha q/2)}$
- They are all mutually unbiased relatively to the eigen states of the position operator because $| < x|\tilde{k}_\alpha > |$ is constant, $\forall k, x \in R$.
- They are also mutually unbiased relatively to each other because whenever $\alpha \neq \alpha'$, one can show that $| < \tilde{k}_\alpha|\tilde{k}'_{\alpha'} > |$ is constant[a] , $\forall k, k' \in R$.

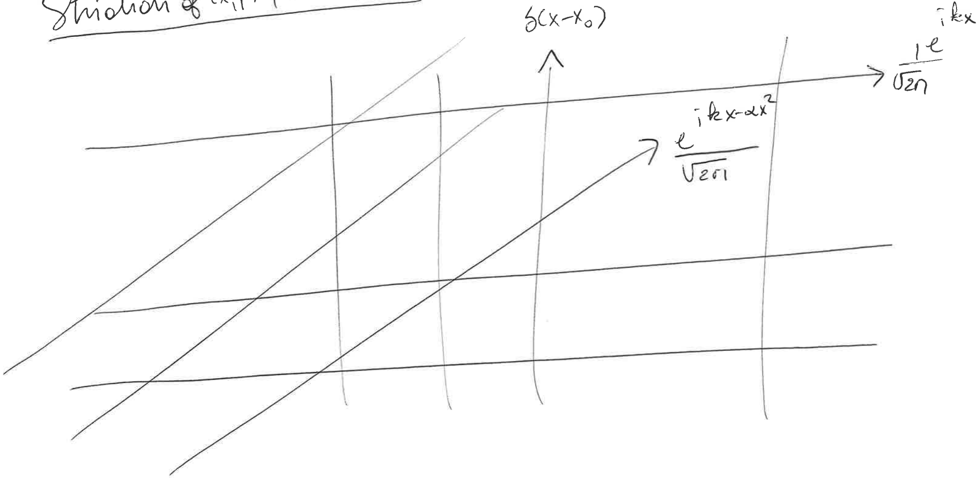
[a] X. Lu, P. Raynal and B-G Englert, PHYSICAL REVIEW A 85, 052316 (2012), Mutually unbiased bases for the rotor degree of freedom.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- Striation and MUB states[a].

Generalized Fourier complementarity and phase-space structure – MARGINALS

Striation of (x,p) phase-space =



-

[a] W. K. Wootters, Ann. Phys. (N.Y.) 176 1 (1987), A Wigner function formalism of finite-state quantum mechanics.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

TOMOGRAPHIC APPLICATIONS: Weyl distribution.

- One can check the following useful identity:
  $|x >< x| = (1/h) \int dp e^{-ipx/\hbar} U_{0,p}$
  Indeed,
  $(1/h) \int dp e^{-ipx/\hbar} U_{0,p} = (1/h) \int dp e^{-ipx/\hbar} e^{ip\hat{x}/\hbar}$
  $= (1/h) \int dp e^{-ipx/\hbar} e^{ip\hat{x}/\hbar} \int d\tilde{x} |\tilde{x} >< \tilde{x}|$
  $=(1/h) \int d\tilde{x} \int dp e^{-ipx/\hbar} e^{ip\tilde{x}/\hbar} |\tilde{x} >< \tilde{x}| =$
  $(1/2\pi) \int d\tilde{x} \int d(p/\hbar) e^{ip(\tilde{x}-x)/\hbar} |\tilde{x} >< \tilde{x}| = |x >< x|;$

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

TOMOGRAPHIC APPLICATIONS: Weyl distribution.

- The identity $|x >< x| = (1/h) \int dp e^{-ipx/\hbar} U_{0,p}$ is the Fourier invert of another useful identity: $U_{0,p} = \int dx e^{ipx/\hbar} |x >< x|$.

  Note that all operators $U_{0,p}$ are diagonal in the position representation.

- Let us now consider an arbitrary direction in phase-space, passing through the origin, parameterised, in dimensionless variables, by the equation

  $p_q - \alpha q = 0$.

- The displacements along this direction are represented by the operators $U_{q,-\alpha q} = e^{i(q\hat{k} - \alpha q \hat{q})}$ where $\hat{k} = (1/i)\frac{\partial}{\partial q}$ in the q representation. They all commute.

- Making use of the aforementioned invariance under symplectic transforms, we get (passing again to dimensionless variables for simplicity)

  $U_{q,-\alpha q} = \int dk e^{ikx} |\tilde{k}_\alpha >< \tilde{k}_\alpha|$ where $|\tilde{k}_\alpha >$ is a generalised plane wave basis.

- The invert Fourier relation reads $|\tilde{k}_\alpha >< \tilde{k}_\alpha| = (1/2\pi) \int dq e^{-ikq} U_{q,-\alpha q}$

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

TOMOGRAPHIC APPLICATIONS: Weyl distribution.

- To estimate the density operator, a possible strategy consists of measuring the transition probabilities in the MUBs, which makes it possible via a Fourier transform to estimate $Tr.(U_{x,p}\rho)$.
- $\rho = (1/h) \int \int dpdq e^{ip\hat{x}/\hbar + ix\hat{p}/\hbar} Tr(e^{(-ip\hat{x}-ix\hat{p})/\hbar}\rho)$

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

TOMOGRAPHIC APPLICATIONS: Weyl distribution.

- Relation between MUBs and Weyl (displacement) operators.

WEYL OPERATORS VERSUS

$\left\{ \begin{array}{l} \text{MUB states} \\ \text{GENERALIZED Fourier states} \end{array} \right.$

$|x\rangle\langle x| = \frac{1}{h}\int dp\, \mathcal{U}(0,p)\, e^{-\frac{ipx}{\hbar}}$

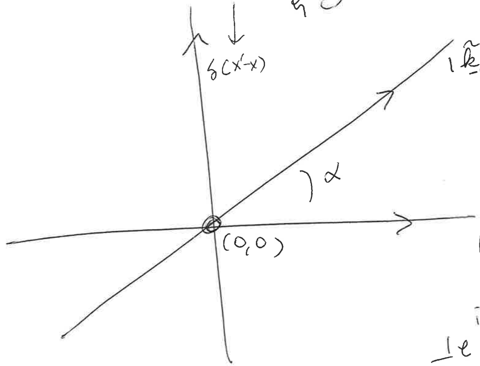
$\downarrow$

$\delta(x'-x)$

$|\tilde{k}_\alpha\rangle\langle\tilde{k}_\alpha| = \frac{1}{2\pi}\int dq\, e^{-ikq}\, \mathcal{U}(q,-\alpha q)$

$\downarrow$

$\frac{1}{\sqrt{2\pi}}\, e^{i(kq-\alpha\frac{q^2}{2})}$



$|\tilde{p}\rangle\langle\tilde{p}| = \frac{1}{h}\int dx\, \mathcal{U}(x,0)\, e^{-\frac{ipx}{\hbar}}$

$\downarrow$

$\frac{1}{\sqrt{2\pi}}\, e^{\frac{ipx}{\hbar}}$

-

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

TOMOGRAPHIC APPLICATIONS: Wigner distribution.

- Another useful identity relates Wigner operators to MUB states: $|x><x| = \int dp W_{x,p}$
- Indeed, having in mind that $(1/h)\int dp e^{-ipx/\hbar} U_{0,p} = |x><x|$, we get

$$\int dp W_{0,p} = \int dp \frac{1}{\hbar^2} \int dx'' dp'' e^{i \frac{(0,p)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} x'' \\ p'' \end{pmatrix}}{\hbar}} U_{x'',p''}$$

$$= (1/h)\int dp \frac{1}{2\pi\hbar} \int dx'' dp'' e^{-i\frac{px''}{\hbar}} U_{x'',p''} = (2\pi/(2\pi h)) \int dp'' \int dx'' \delta^{Dirac}_{x''} U_{x'',p''}$$

$$= (1/h)\int dp U_{0,p} = |x=0><x=0|;$$

making use of property 2 (Wigner distribution transforms “naturally” under Galilean transformations), we finally get

$|x><x| = \int dp W_{x,p}$ which is directly related to the marginal property.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

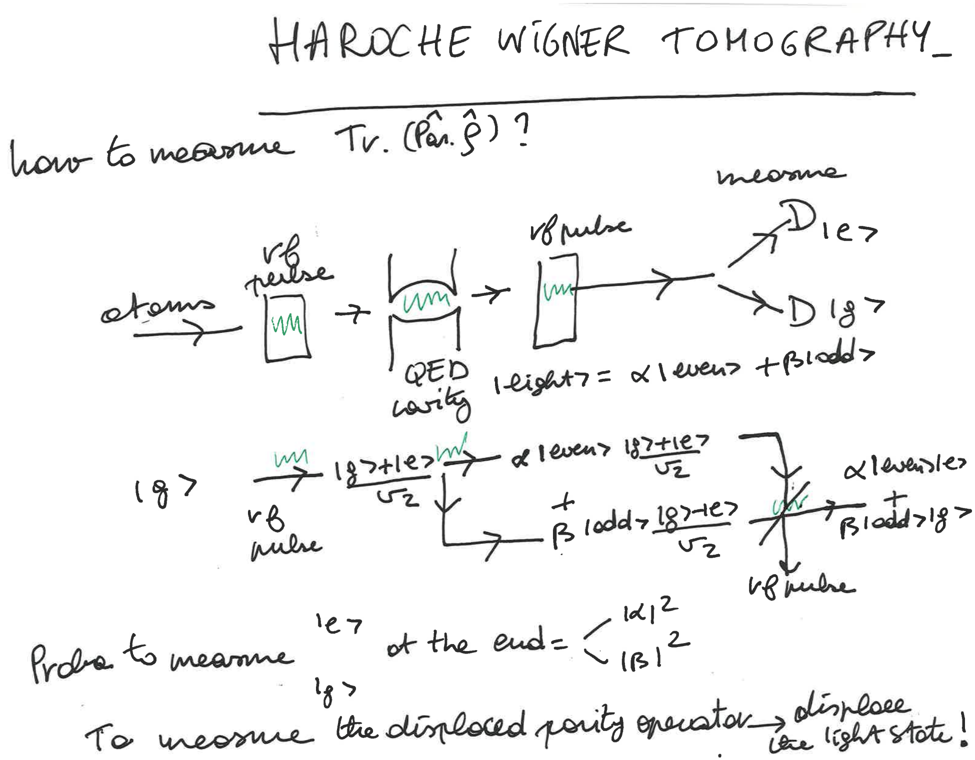
TOMOGRAPHIC APPLICATIONS: Wigner distribution.

- In $\mathcal{L}^2(\mathbb{R})$, if we wish to perform Wigner tomography of an unknown quantum state, there is, a priori[a], no gain in measuring the transition probabilities to the basis states associated to the striation of the phase-space.
- **A succesful strategy consists of directly measuring the average values of the Wigner operators; this has been done by the team of Serge Haroche (Nobel prize 2012).**

[a] This is no longer so in finite dimensions, as we shall see.

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- Haroche Wigner tomography via entangled atoms passing through a QED cavity.

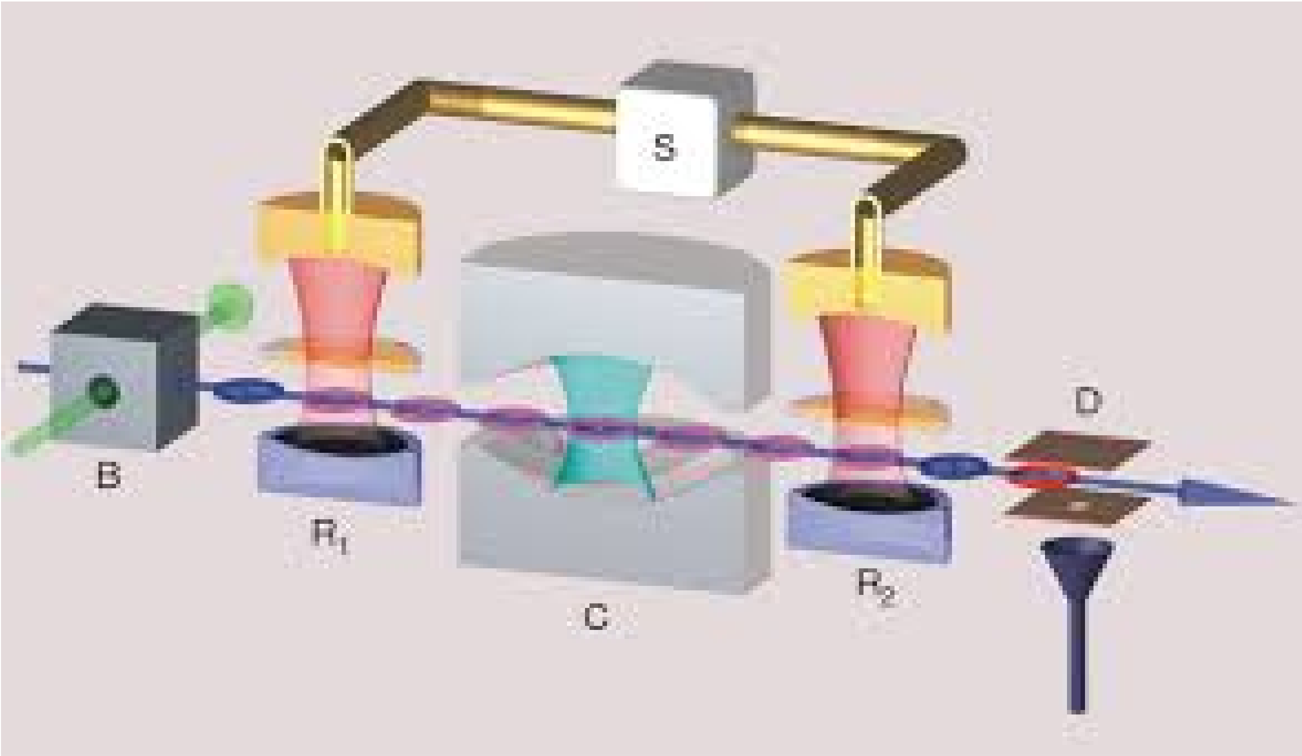


-

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- Haroche Wigner tomography via entangled atoms passing through a QED cavity[a]

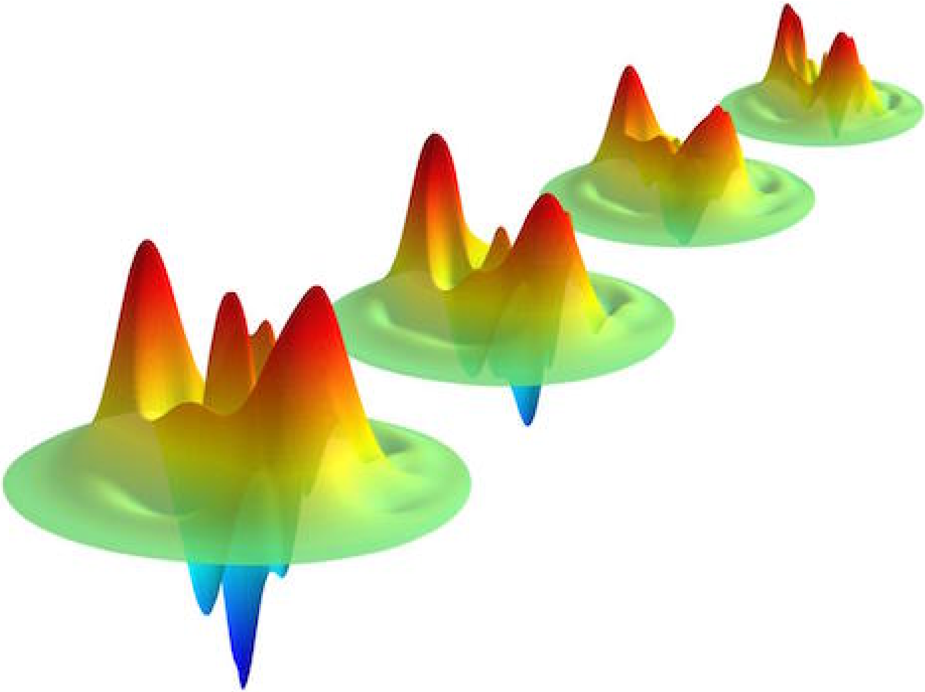
-



[a]http://www.lkb.upmc.fr/cqed/wp-content/uploads/sites/14/2016/06/2009-LKB-AERES-StateReconstruction_low.pdf

H-W group in $\mathcal{L}^2(\mathbb{R})$: applications.

- Haroche Wigner tomography: movie of decoherence of a cat state in a lossy cavity QED[a].



-

[a] http://www.lkb.upmc.fr/cqed/non-local-quantum-states/

Finite dimensions.

Passing from the continuum to finite dim. d: discretization.

- All aforementioned properties are integrally preserved in d dimensional Hilbert spaces provided d is a prime power[a]: $d = p^m$, with p prime and m a positive integer[b].

[a] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) 191, 363 (1989), Optimal state-determination by mutually unbiased measurements, K. S. Gibbons, M. J. Hoffman and W. K. Wootters, Phys. Rev. A 70 062101 (2004), Discrete phase space based on finite fields.

[b] T. Durt, B-G Englert, I. Bengtsson, and K. Zyczkowski: IJQI, vol. 8, nr 4, 535-640 (2010), On mutually unbiased bases.

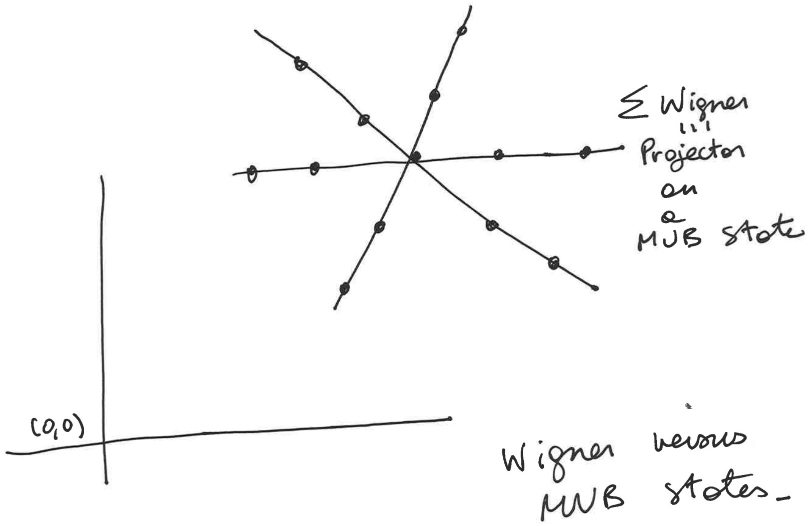
Prime power dimensions: $d = p^m$.

The main properties are listed below:

- There exist $d + 1$ MUBs.
- MUB states are eigenstates of the (discrete) Heisenberg-Weyl operators (phase-space displacement operators).
- To each MUB corresponds a set of d parallel straight lines, each of them corresponding to a MUB state.
- Two different MUB states are either associated to parallel lines (if they belong to the same MUB) or to non-parallel lines (otherwise) which intersect in one point in phase-space; this represents the overlap between states from different MUBs (which is equal to $1/\sqrt{d}$ in modulus).
- To each point in the d^2 dimensional phase-space we can associate a phase-space localisation operator (Wigner operator).
- **Moreover, in prime power dimensions, this Wigner operator is equal to the sum of the projectors onto MUB states associated to straight lines passing through that point minus the identity, divided by d.**

Prime power dimensions: $d = p^m$.

- Wigner (phase-space localisation) operators and MUB states.



Same as in $\mathcal{L}_2(\mathbb{R})$ but now with a
DISCRETE PHASE SPACE.

Dimensional dependency.

What is special with prime power dimensions?

- The key ingredient is the existence of a finite field with d elements (Galois showed in the 19th century that finite fields exist if and only their cardinality is a prime power).
- Let us denote $\oplus_G$ and $\odot_G$ the corresponding operations.
- In prime dimensions they are nothing else than the cyclic addition and multiplication, that is to say, addition and multiplication modulo d and expressions of MUBs are easy to tackle[a]..
- In prime power but non-prime dimensions ($d = p^m$, $m \neq 1$), the situation is more involved.
- Let us consider for instance $d = 4$...

[a] Ivanovic, Geometrical description of quantal state determination, Phys.A:Math.Gen.143241, 1981.

Dimensional dependency.

What is special with prime power dimensions?, APARTE: Dimension 4.

- There exist, in dimension 4, 4.3.2=24 permutations between states from a same basis. Two subgroups of this group of 24 elements are particularly interesting (see picture next page):

- The cyclic group with 4 elements generated by the permutation
  $P_1 = |0\rangle \to |1\rangle; |1\rangle \to |2\rangle; |2\rangle \to |3\rangle; |3\rangle \to |4\rangle.$
  It also contains the identity P_0, and the power 2 and 3 of the generator:
  $P_2 = |0\rangle \to |2\rangle; |1\rangle \to |3\rangle; |2\rangle \to |0\rangle; |3\rangle \to |1\rangle.$
  $P_3 = |0\rangle \to |3\rangle; |1\rangle \to |0\rangle; |2\rangle \to |1\rangle; |3\rangle \to |2\rangle.$

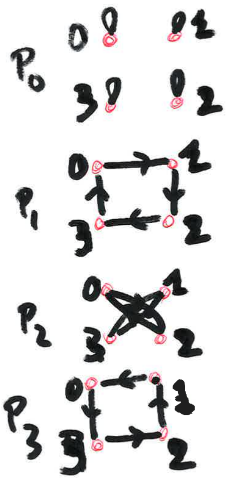
- The "Galois" group that contains the identity and the 3 following permutations:
  $P_2' = |0\rangle \to |2\rangle; |1\rangle \to |3\rangle; |2\rangle \to |0\rangle; |3\rangle \to |1\rangle.$
  $P_1' = |0\rangle \to |1\rangle; |1\rangle \to |0\rangle; |2\rangle \to |3\rangle; |3\rangle \to |2\rangle.$
  $P_3' = |0\rangle \to |3\rangle; |1\rangle \to |2\rangle; |2\rangle \to |1\rangle; |3\rangle \to |0\rangle.$

Dimensional dependency.

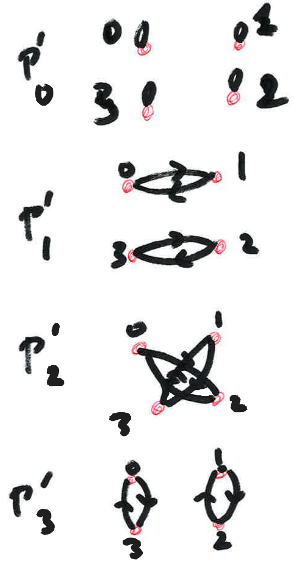
What is special with prime power dimensions?, APARTE: Dimension 4.

Two interesting groups of permutations of 4 objects (of cardinality 4):

"Cyclic" group



"Galois" group



Dimensional dependency.

What is special with prime power dimensions?, APARTE: Dimension 4.
On the basis of the composition law of these (commutative) groups it is easy to define a (commutative) addition law through the relation
$P_i.P_j = P_{i+j}$ $(i, j = 0, 1, 2, 3)$.
We find so the following addition tables:

$$\begin{array}{ccccc} +_{cycl.} . & 0. & 1. & 2. & 3. \\ 0. & 0 & 1 & 2 & 3 \\ 1. & 1 & 2 & 3 & 0 \\ 2. & 2 & 3 & 0 & 1 \\ 3. & 3 & 0 & 1 & 2 \end{array} \tag{7}$$

$$\begin{array}{ccccc} \oplus_G . & 0. & 1. & 2. & 3. \\ 0. & 0 & 1 & 2 & 3 \\ 1. & 1 & 0 & 3 & 2 \\ 2. & 2 & 3 & 0 & 1 \\ 3. & 3 & 2 & 1 & 0 \end{array} \tag{8}$$

Dimensional dependency.

What is special with prime power dimensions?, APARTE: Dimension 4.

On the basis of these addition tables it is also easy to define a (commutative) multiplication law that is distributive relatively to the addition:,

We find so the following multiplication tables:

$$\begin{array}{ccccc} \cdot_{cycl.}\cdot & 0. & 1. & 2. & 3. \\ 0. & 0 & 0 & 0 & 0 \\ 1. & 0 & 1 & 2 & 3 \\ 2. & 0 & 2 & 0 & 2 \\ 3. & 0 & 3 & 2 & 1 \end{array} \tag{9}$$

Remark:

The addition and the “cyclic” multiplication are nothing else than the MODULO 4 addition and multiplication.

Dimensional dependency.

What is special with prime power dimensions?, APARTE: Dimension 4.
The Galois multiplication table is the following:

$$\begin{array}{ccccc} \odot_G . & 0. & 1. & 2. & 3. \\ 0. & 0 & 0 & 0 & 0 \\ 1. & 0 & 1 & 2 & 3 \\ 2. & 0 & 2 & 3 & 1 \\ 3. & 0 & 3 & 1 & 2 \end{array} \qquad (10)$$

- Such algebraic structures are called "COMMUTATIVE RINGS";
  the Galois multiplication is moreover endowed with a remarkable property:
  THERE IS NO DIVIDER OF ZERO, EXCEPTED ZERO ITSELF...
- Therefore the Galois ring is also called a FIELD (finite field). In french fields are called corps.
- Evariste Galois derived in the 19th century atechnique for generating such addition and multiplication d times d tables for arbitrary prime power values of d.
- No finite field exists of cardinality different from p^m...

Dimensional dependency.

What is special with prime power dimensions?

- As already mentioned, in prime power dimensions, the same properties as those described in the continuous case regarding MUBs, Wigner operators and so on are valid.
- They can be established by direct construction (**constructive approach**).
- The key ingredient is the existence of a finite field with d elements endowed with an addition$\oplus_G$ and a multiplication $\odot_G$.
- Because there is no dividor of 0, the neutral for addition, in a field, excepted 0, the set of equations $a \odot x + b \odot y = c$ defines an **affine** structuration of the (x, p) plane such that there exist $d + 1$ sets of d parallel lines for which affine axioms are satisfied:

  -two distinct parallel lines have no point in common

  -two non-parallel lines intersect in only one point

  -each point belongs to $d + 1$ non-parallel lines and so on...

Dimensional dependency.

What is special with prime power dimensions?

- One can also show that:

$$\sum_{j=0}^{d-1} \gamma_G^{(j \odot_G i)} = d\delta_{i,0} \tag{11}$$

$$\gamma_G^i \cdot \gamma_G^j = \gamma_G^{(i \oplus_G j)} \tag{12}$$

where $\gamma_G$is a well-chosen phase (pth root of unity: $\gamma_G = e^{i.2\pi/p}$).

- These identities are the basis of all the calculus necessary for characterizing MUBs in prime power dimensions.

Dimensional dependency.

What is special with prime power dimensions?

- Besides, the Galois addition factorizes; for instance, in dimension 4, if we express quartits like tensorial products of 2 qubits: $|0\rangle_4 = |0\rangle_2 \otimes |0\rangle_2$, $|1\rangle_4 = |0\rangle_2 \otimes |1\rangle_2$, $|2\rangle_4 = |1\rangle_2 \otimes |0\rangle_2$, $|3\rangle_4 = |1\rangle_2 \otimes |1\rangle_2$,we can check at the level of the addition table that

  if $|i\rangle_4 = |i_1\rangle_2 \otimes |i_2\rangle_2$, et $|j\rangle_4 = |j_1\rangle_2 \otimes |j_2\rangle_2$,

  then $|i \oplus_G j\rangle_4 = |i_1 \oplus_{mod2} j_1\rangle_2 \otimes |i_2 \oplus_{mod2} j_2\rangle_2$.

- This means that the (quartit here) addition FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE. In dimension p^m, the Galois addition always FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE.

- The Galois multiplication table is more involved.

Dimensional dependency.

What is special with prime power dimensions?

- Remark:

  Some of these properties generalize to the displacement operators that are defined through the MODULO operations:

- Example:

$$\sum_{j=0}^{d-1} \gamma_{mod.}^{(j \cdot_{mod.} i)} = d\delta_{i,0} \tag{13}$$

$$\gamma_{mod.}^{i} \cdot \gamma_{mod.}^{j} = \gamma_{mod.}^{(i +_{mod.} j)} \tag{14}$$

- Here $\gamma_{mod.}$ is the dth root of unity: $\gamma_{mod.} = e^{i.2\pi/d}$.

- In both cases, calculus is made possible in virtue of the properties above[a].

[a] T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283.

Dimensional dependency.

What is special with prime power dimensions?

- In prime power dimensions, it is possible to build $d+1$ MUBs by the same technique as in the continuum.
- On the basis of the field operations, one can now define discrete displacement operatorsoperators: the generalised Pauli or Heisenberg-Weyl group which constitutes a discrete version of their continuous counterpart studied before.
- Such operators are can be defined as follows[a]:

$$V_i^j = \sum_{k=0}^{d-1} \gamma_G^{((k \oplus_G i) \odot_G j)} |k \oplus_G i\rangle\langle k|, \tag{15}$$

[a] T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283.

Dimensional dependency.

What is special with prime power dimensions?

- We can derive $d+1$ MUBs by simultaneously diagonalising well-chosen subgroups of the generalized Pauli group ($V_l^{(\alpha \odot_G l)}$, equal to $U_{l,\alpha \odot_G l}$ up to a global phase factor[a]).

- We found for instance that in odd prime power dimension p^m (with p a prime diferent from 2), MUBs can be expressed as follows[b]:

$$|\tilde{e}_k^i\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \gamma_G^{\ominus_G q \odot_G k} (\gamma_G^{((\alpha \odot_G q \odot_G q)/_G 2)}) |e_q^0\rangle, \tag{16}$$

  where the states of the generalized Fourier bases are denoted $|\tilde{e}_k^i\rangle$ and those of the so-called computational basis (the discrete analog of the X basis) are denoted $|e_q^0\rangle$.

[a]This phase is fixed by requiring that the U operators form a group: $U_{l_1,\alpha \odot_G l_1}.U_{l_2,\alpha \odot_G l_2}$=$U_{l_1 \oplus l_2,\alpha \odot_G (l_1 \oplus l_2,)}$. In odd prime power dimensions for instance, we find $U_{m,n} = \gamma^{m \odot_G n/_G 2} V_{m,n}$, very similar to its counterpart in the case of the continuum.

[b]T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283.

Dimensional dependency.

What is special with prime power dimensions?

- Warning:

  the parameterization chosen in the case of finite dim. Hilbert spaces leads to the inverse Fourier transform instead of the Fourier transform. It is not difficult to choose parameterizations that would exhibit more consistency when passing to the limit of the continuum. We will not do it however because this would breal consistency with many bibliographic references.

Dimensional dependency.

What is special with prime power dimensions?

- Remark:

  -In even prime power dimensions (2^m m qubits), things is more complicated, as is well-known: even and odd cardinality finite fields are totally different; we find[a]:

$$|\tilde{e}_j^l\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \gamma_G^{\ominus_G k \odot_G k} \alpha_{\ominus k}^j \tag{17}$$

where $\alpha_l^j = \prod_{q,n=0}^{m-1} i^{(j \odot_G (l_q 2^q) \odot_G (l_n \odot 2^n))}$ with $l = \sum_{n=0}^{m-1} l_n 2^n = \sum_{q=0}^{m-1} l_q 2^q$.

[a] T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283, A. Eusebi and S. Mancini, "Deterministic quantum distribution of a d-ary key ", Quant. Inf. Comp. 9 (2009) 950, T. Durt, B-G Englert, I. Bengtsson, and K. Zyczkowski: "On mutually unbiased bases", IJQI, vol. 8, nr 4, 535-640 (2010).

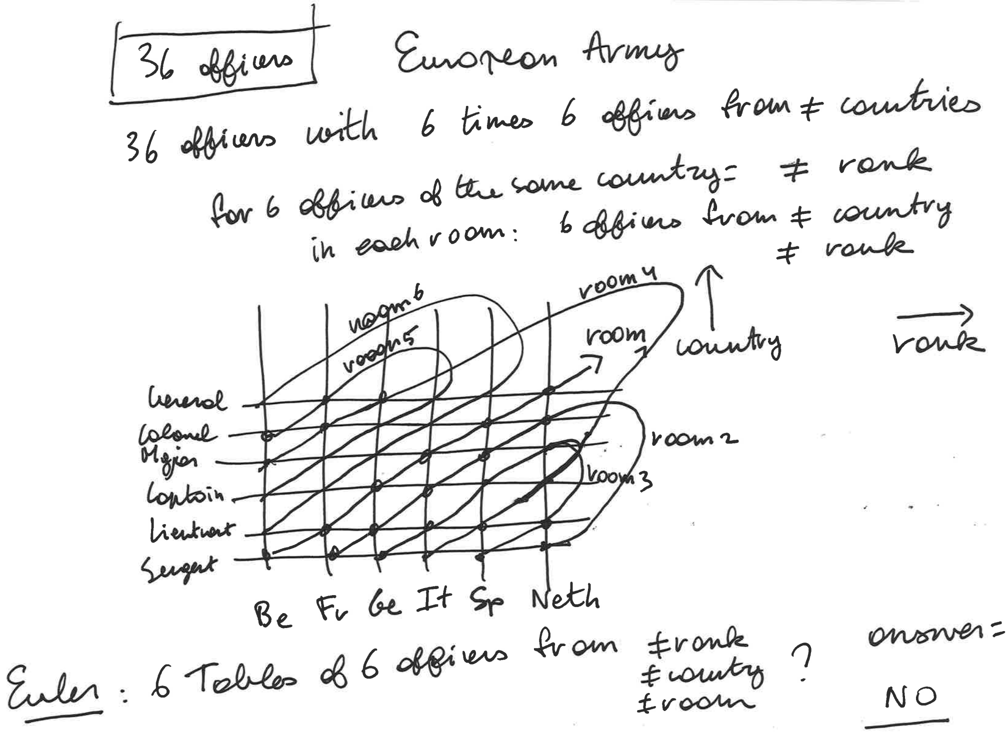
Application: quantum tomography in prime power dimension $d = p^m$.

- As there are $d+1$ MUBs in dimension $d = p^m$, that each von Neumann-measurement of an operator diagonal in a MUB provides $d-1$ independent parameters, and that the results collected in different MUBs are also independent, we get $d^2 - 1$ independent parameters.
- This is precisely equal to the number of independent parameters that are necessary in order to reconstruct the density matrix of an unknown d-level quantum state. We can thus perform a FULL TOMOGRAPHIC process by measuring transition probabilities in $d+1$ MUBs.
- Example: $d = 2$: we get the $d^2 - 1 = 3$ Bloch (Stokes) coefficients by measuring the transition probabilities in 3 MUBs (in polarimetry: we measure the populations of circular left and right polarisations, horizontal-vertical and diagonal.)

Dimensional dependency.

What about other (non prime-power) dimensions?

- In dimension 6, no affine plane exists[a], in relation with Euler's conjecture concerning the problem of the 36 officers.



-

[a]Tarry G 1900 C. R. Assoc. Fr. Av. Sci. Natl 1 122, 2170

Dimensional dependency.

What about other (non prime-power) dimensions?

- *...Progress since the work of Tarry in 1900 has been slow*[a]*. Finite affine planes do NOT exist if* $d = 4k + 1$ *or* $d = 4k + 2$ *and* d *is not the sum of two squares or if* $d = 10$*....*
- It is conjectured that affine planes only exist when d is a prime power.
- It is also conjectured that maximal sets of $d + 1$ MUBs only exist in prime power dimensions.
- Another conjecture concerns the maximal number of MUBs in non prime power dimensions[b]: it would be equal to the maximal number of different directions in a d times d plane satisfying the postulates of affine geometry (3 in the case of MUBs).
- Let us now focus on dimensions 2 and 3.

---

[a] M. Appleby, I. Begtsson and M. Chaturvedy, Journal of Mathematical Physics 49, 012102 (2008), Spectra of phase point operators in odd prime dimensions and the extended Clifford group.

[b] M. Saniga, M. Planat and H. Rosu, J. Opt. Quantum Semiclass. B6, L19 (2004), Mutually unbiased bases and finite projective planes, T. Durt and S. Weigert, J. Phys. A: Math. Theor. 43 402002, 2010, Affine constellations without mutually unbiased counterparts.

QUBITS (d=2), permutations versus displacement operators in the qubit space.

- Most simple case: two-level systems (QUBITS): d=2.
- Two possible permutations: the identity and the negation (exchange of 0 and 1) which permutes the qubit basis state $|0\rangle$ with $|1\rangle$.
- We can express the identity by the identity operator $|0\rangle\langle 0| + |1\rangle\langle 1|$.
- The operator associated to the negation can be written $|1\rangle\langle 0| + |0\rangle\langle 1|$.
- When $|0\rangle$ and $|1\rangle$ correspond to the North and South poles of the Stokes-Poincare-Bloch sphere: (along the Z axis: $|0\rangle$=$|+\rangle_Z$; $|1\rangle$=$|-\rangle_Z$), this operator is equal to the Pauli σ_x operator itself!
- This operator is diagonal in the basis $(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$.

QUBITS (d=2),

displacement operators in the qubit space.

- We can now repeat the reasoning and consider the two possible permutations of the eigenstates of σ_x.
- We find then the identity operator while the operator that corresponds to the negation is equal to $|0\rangle\langle 0| - |1\rangle\langle 1|$.
- When $|0\rangle$ and $|1\rangle$correspond to the North and South poles (along Z), this operator is the Pauli operator σ_z!
- The composition of the operators σ_z et σ_x is equal, up to a global phase[a], to σ_y.
- σ_y is diagonal in the basis $(\frac{1}{\sqrt{2}}(|0\rangle + i.|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle))$.
- We find so the 4 Pauli operators:, the identity and the 3 σ operators.

[a] This phase is fixed by imposing that the corresponding displacement operator is self-adjoint. Here we find $U_{0,1} = V_{0,1} = \sigma_Z$, $U_{1,0} = V_{1,0} = \sigma_X$, and $U_{1,1} = iV_{1,1} = \sigma_Y$

3 MUBs in the qubit space.

- Such operators form a group (up to global phases), the Pauli group. It is the qubit counterpart of the Heisenberg-Weyl group.
- This group itself consists of 3 subgroups which consist of the identity and one of the 3 operators $\sigma_{x,y,z}$. These 3 subgroups are diagonal in the bases:
  $(|0\rangle, |1\rangle)$
  $(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$
  and $(\frac{1}{\sqrt{2}}(|0\rangle + i.|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle))$.
- Such bases are said to be "mutually unbiased" (MUBs):

  Definition: "A collection of orthonormal bases of a d dimensional Hilbert space is said to be mutually unbiased if whenever we choose two states from different bases, the modulus squared of their in-product is equal to $1/d$. "

- The transition probabilities between states from different MUBs are all equal to $1/d$ (in the qubit case they are 50-50 probabilities as when we toss an UNBIASED COIN).

Pauli displacement operators.

and (Bloch) tomography.

- Pauli operators form an orthonormalised basis of the linear operators (relatively to the Trace-norm product).
- As a consequence, any qubit DENSITY MATRIX or density operator is a linear combination of Pauli operators:
  $\hat{\rho} = \frac{1}{2}(\sigma_0 + k_x\sigma_x + k_y\sigma_y + k_z\sigma_z)$.
  We recognize here Bloch parameters (NMR) or Stokes-Jones-Poincaré parameters (polarimetry).
- In order to estimate these parameters it is enough to measure the transition probabilities in the 3 corresponding bases (MUBs).
- By doing so we realize a QUANTUM TOMOGRAPHIC PROCESS so to say we can estimate the qubit quantum state.

Remarks.

- The tomographic procedure based on MUBs is OPTIMAL because there is NO REDUNDANCY between data collected in different bases;

  the information is thus never wasted during the data acquisition, and there is no redundancy in the acquisition.

- MUBs are a manifestation of complementarity.

Application: Wigner distribution in the qubit case (dimension 2).

- The qubit Wigner distribution is equal to the average value of Wigner operators.
- It is not clear however what would be the counterpart of the parity operator in dimension 2 because $0 = -0$ modulo 2 and $1 = -1$ modulo 2.
- The discrete parity operator is however defined unambiguously by the discrete version of the identity $P\hat{a}r. = \frac{1}{2h} \int dxdpU_{x,p}$. which reads

  $P\hat{a}r. = 1/d^2 \sum_{m,n \in 0,1...d-1} U_{m,n}$
- Applying this property and deriving the all Wigner operators after displacing W_{00} in the 2 times 2 phase-space, we find the Wigner distribution (expressed in function of Bloch-Stokes parameters defined through $\vec{k} =< \vec{\sigma} >$)

$$\begin{cases} w_{00} = \frac{1}{4}\left[1 + k_x + k_y + k_z\right] \\ w_{01} = \frac{1}{4}\left[1 - k_x - k_y + k_z\right] \\ w_{10} = \frac{1}{4}\left[1 + k_x - k_y - k_z\right] \\ w_{11} = \frac{1}{4}\left[1 - k_x + k_y - k_z\right] \end{cases} \tag{18}$$

Application: Wigner distribution in the qubit case (dimension 2).

- As their continuous counterparts the Wigner operators obey the following constraints[a]:

  (a) Translational invariance: $W_{(i_1,i_2)} = (V_{i_1}^{i_2})^\dagger W_{(0,0)} V_{i_1}^{i_2}$;

  (b) The sum of the $d^2 = 4$ Wigner amplitudes $Tr.\hat{\rho}.W_{(i_1,i_2)}$ is normalized to unity;

  (c) Marginals: if we consider STRAIGHT LINES in phase-space defined by the relations $a \odot_G i_1 = b \odot_G i_2 \oplus_G c$, with a b and c elements of the finite Galois field with 2 elements ($\{0, 1\}$), where addition and multiplication are defined modulo 2, the averages of Wigner operators along such lines (marginals) are equal to a projector onto one of the MUBs states.

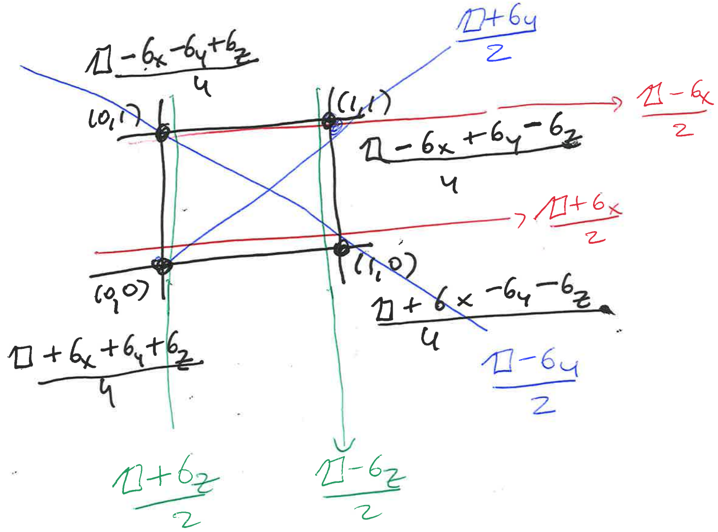
- Moreover, marginals along non-intersecting parallel lines correspond to projectors onto orthogonal states of a same MUB while marginals taken along non-parallel directions correspond to projectors onto states from different MUBs.

[a] W. K. Wootters, Ann. Phys. (N.Y.) 176 1 (1987), A wigner function formalism of finite-state quantum mechanics.

Qubit Wigner operators.

QUBIT WIGNER OPERATORS

and their MARGINALS (Wootters'87.)



Qubit Wigner operators.

- Moreover the following property, valid in finite dimension only, delivers an alternative definition of the Wigner operators[a]:

  ... the Wigner operator in a point (x, p) is proportional to the sum of the projectors onto all MUB states related to straight lines passing through that point minus the identity operator[a]*...*

[a] M. Appleby, I. Begtsson and M. Chaturvedy, Journal of Mathematical Physics 49, 012102 (2008), Spectra of phase point operators in odd prime dimensions and the extended Clifford group.

Qubit Wigner operators.

- Proof:

  the Wigner operator at the origin is equal to the parity operator:

  $P\hat{a}r. = 1/d^2 \sum_{m,n \in 0,1 \ldots d-1} U_{m,n}$

  Integrating along straight lines in the finite phase-space, and making use of the identities

  $\sum_{n \in 0,1 \ldots d-1} U_{0,n} = d|e_0^0 >< e_0^0|$ and

  $\sum_{m \in \{0,1 \ldots d-1\}} U_{m,\alpha m} = d|\tilde{e}_0^\alpha >< \tilde{e}_0^\alpha|$,

  we find that the Wigner operator at the origin is equal to $1/d$ times the sum of the projectors on the 0th basis states of the $d+1$ MUBs minus d times U_{00}. This is so because we counted U_{00} in the summation $d+1$ times and not only once. Now, the null displacement U_{00} is equal to the identity operator so that we finally obtain the following identity (only valid in finite prime power dimensions):

  $\hat{W}_{00} = P\hat{a}r. = (1/d)(|e_0^0 >< e_0^0| + \sum_{\alpha \in \{0,d-1\}} |\tilde{e}_0^\alpha >< \tilde{e}_0^\alpha| - U_{00})$

  $= (1/d)(|e_0^0 >< e_0^0| + \sum_{\alpha \in \{0,d-1\}} |\tilde{e}_0^\alpha >< \tilde{e}_0^\alpha| - Identity)$

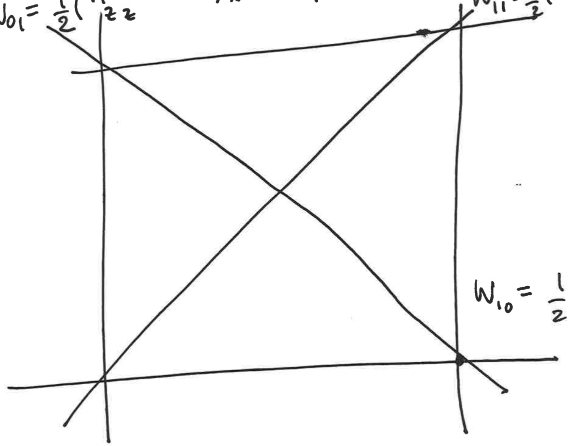
- Other Wigner operators are obtained in a similar fashion by displacing the "parity" operator.

Qubit Wigner operators.

Wigner Operators and MUB states. (BIS)

$$W_{01} = \frac{1}{2}\left(|+\rangle_z\langle +|_z + |-\rangle_x\langle -|_x + |-\rangle_y\langle -|_y - \mathbb{1} \right)$$

$$W_{11} = \frac{1}{2}\left(|-\rangle_z\langle -|_z + |-\rangle_x\langle -|_x + |+\rangle_y\langle +|_y - \mathbb{1} \right)$$



$$W_{10} = \frac{1}{2}\left(|-\rangle_z\langle -|_z + |+\rangle_x\langle +|_x + |-\rangle_y\langle -|_y - \mathbb{1} \right)$$

$$W_{00} = \frac{1}{2}\left(|+\rangle_z\langle +|_z + |+\rangle_x\langle +|_x + |+\rangle_y\langle +|_y - \mathbb{1} \right)$$

Qubit Wigner operators.

- In particular the qubit counterpart of the parity operator reads
  $\hat{W}_{00} = (1/2)(|+>_X< +|_X + |+>_Y< +|_Y + |+>_Z< +|_Z - Identity)$,
  in agreement with a previously derived identity
  $w_{00} = \frac{1}{4}\left[1 + k_x + k_y + k_z\right]$

QUTRITS (d=3),

MUBs in the qutrit space.

- The Heisenberg-Weyl group counts 9 operators and is constructed by combining translations and boosts.

$$V_i^j = \sum_{k=0}^{d-1=2} \gamma_G^{((k \oplus_G i) \odot_G j)} |k \oplus_G i\rangle\langle k|, \tag{19}$$

  where the Galois operations are addition and multiplication modulo 3.

- It counts 4 commuting subgroups, each of them being related to a direction in the 3 times 3 phase space.
- Those subgroups are diagonal in 4 MUBs.

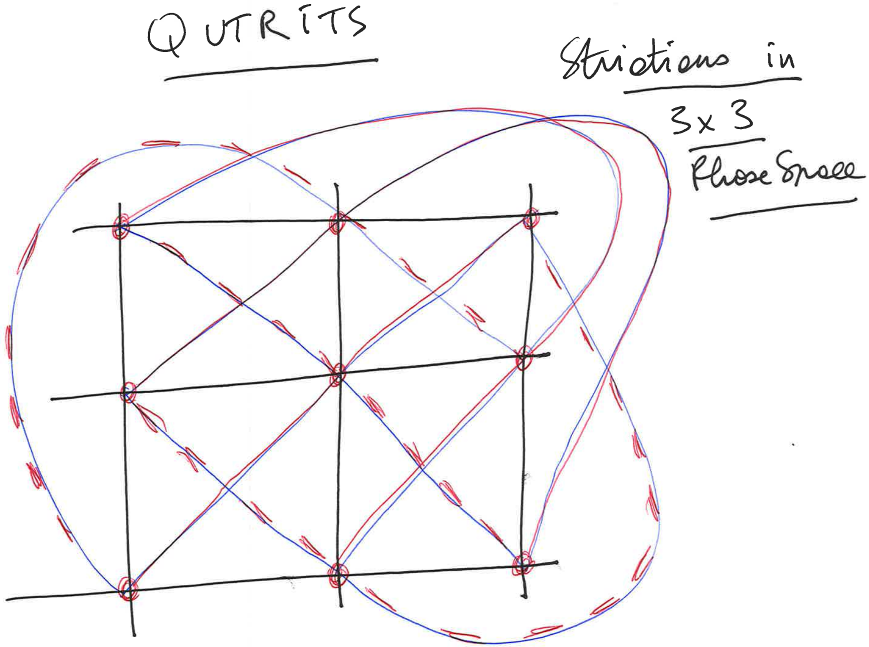
QUTRITS (d=3),

MUBs in the qutrit space.

- Let us represent each MUB by a 3 times 3 matrix via the following recipe -the states of the computational basis $|e_0^0>$, $|e_1^0>$ and $|e_2^0>$ corresponds to the column matrices $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$;
- we represent a MUB by a 3 times 3 matrix each column of which represents a MUB state; the subgroup of vertical displacements is diagonal in the computational basis, represented by the identity matrix; the subgroup of horizontal displacements is diagonal in the Fourier basis; this corresponds to the two first matrices given below;
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & \gamma & \gamma^2 \\ 1 & \gamma^2 & \gamma \end{pmatrix},$$
- the two other directions are associated to the two last matrices given below:
$$\begin{pmatrix} 1 & 1 & 1 \\ \gamma & \gamma^2 & 1 \\ \gamma & 1 & \gamma^2 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ \gamma^2 & 1 & \gamma \\ \gamma^2 & \gamma & 1 \end{pmatrix}.$$

Qutrit phase-space.

- The 4 MUBs correspond to directions in the 3 times 3 affine phase-space.



-

QUTRITS (d=3),

Wigner operators in the qutrit space.

- As already shown,
  $\hat{W}_{00} = \hat{Par.} = 1/d^2 \sum_{m,n \in 0,1...d-1} U_{m,n}$
  $= (1/d)(|e_0^0 >< e_0^0| + \sum_{\alpha \in \{0,d-1\}} |\tilde{e}_0^\alpha >< \tilde{e}_0^\alpha| - Identity)$
- Other Wigner operators are obtained in a similar fashion by displacing $\hat{W}_{00}$.
- Moreover $\hat{W}_{00}$ is a real parity operator (as is true in all odd dimensions actually):

  -for instance, if we represent the states of the computational basis $|e_0^0 >$, $|e_1^0 >$ and $|e_2^0 >$ by the column matrices $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, then the Wigner operator $\hat{W}_{00}$ corresponds to the matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

SIC POVMs.

- We shall terminate this lesson by presenting a new tomographic technique, related to the Heisenberg-Weyl group defined through the modulo d operations, conjectured to be valid in arbitrary dimension, called SIC tomography.
- **It has the merit to "work" in all dimensions, for instance in dimensions 6, 10 and so on.**
- In particular we shall consider Heisenberg-Weyl covariant SIC POVMs with a focus on dimensions 2 (qubits) and 3 (qutrits).

SIC POVMs.

PVM versus POVM tomography.

- Traditionally, when we measure an observable we carry out a PVM measurement.
- Example: A measurement of an observable diagonal in the X, Y or Z basis is called a Projective-Valued-Measure (PVM) measurement because the probability of firing of a detector is equal to the average value of a projector: $P(+/-)_{X,Y,Z} = Tr.\rho.|+/-\rangle_{X,Y,Z}\langle +/-|_{X,Y,Z}$
- During PVM qubit tomography, the three parameters k_x, k_y and k_z that characterize the state ρ of the qubit are estimated by performing 3 projective (PVM) measurements (one measures the transition probabilities in 3 bases (X,Y, and Z)).
- In the case of polarised photons, for instance, the Stokes-Jones parameters are estimated by successively measuring the degree of polarisation in 3 polarisation bases (horizontal-vertical, diagonal45-diagonal135 and circular left-right).

SIC POVMs.

PVM versus POVM tomography.

- The PVM measurements are a sub-class of more general measurement processes called POVM (Positive Operator Valued Measure) measurements.
- In order to realize a POVM measurement it is sufficient to couple the quantum system to another quantum system (called an ancilla), to entangle them, and to realize a PVM measurement onto the full system: original system plus ancilla.
- If we only consider the effect of this process at the level of the original system (that we obtain by tracing out the ancilla), what we get is called a POVM measurement.

SIC POVMs.

PVM versus POVM tomography.

- In order to realize POVM tomography of a qubit, we couple it to an ancilla of same dimensionality and let them evolve together in such a way that they become entangled with each other.
- For the initial state of the system $|\psi^S\rangle = \sum_{i=0}^{1} \psi_i |e_i^S\rangle$ and the initial state of the ancilla $|e_0^A\rangle$,

  the most general coherent unitary evolution will map their state onto the state $U^{S-A}|\psi^S\rangle|e_0^A\rangle = \sum_{i=0}^{1} \psi_i U^{S-A}|e_i^S\rangle|e_0^A\rangle = \sum_{i,k,j=0}^{d-1} \psi_i U_{k,j}^i |e_k^S\rangle|e_j^A\rangle$.
- In the latter equality, the coefficients $U_{k,j}^i$ are unambiguously determined by the specific unitary evolution U that is imposed to the system.

SIC POVMs.

- If we now perform a joint-measurement in the product-basis $|e_k^S\rangle|e_j^A\rangle$, the d^2 probabilities of firing of the detectors k and j are equal to $|\sum_{i=0}^{1} U_{k,j}^i \psi_i|^2$, where $k, j = 0, d-1$.
- Obviously this probability is in turn equal to the modulus square of the inner product of the initial state $|\psi^S\rangle$ with the (not necessarily normalised) state $|U_{k,j}^S\rangle = \sum_{i=0}^{d-1} U_{k,j}^i |e_i^S\rangle$.
- This is the average value of a Positive Operator, not necessarily a projector, from there the name POVM measure.
- One can show[a] that the optimal POVM tomography corresponds to the situation where the d^2 states $|U_{k,j}^S\rangle$ are treated on the same footing and maximally independent.
- In the practice, this imposes that the scal product between the d^2 states defining the POVM is equal to $\sqrt{1/(d+1)}$.
- Such a POVM is called SIC (Symmetric Informationally Complete) POVM.

[a] A. E. Allahverdyan, R. Balian, and Th. M. Nieuwenhuizen, $Phys. Rev. Lett.$, **92**, 120402 (2004), J. Rehacek, B-G Englert, D. Kaszlikowski, $Phys. Rev. A$, **70**, 052321 (2004)

SIC POVMs.

- In a Hilbert space of dimension d any SIC POVM is thus in one to one correspondence with an equiangular set of d^2 pure states (with in general COMPLEX amplitudes) that we shall call C-d^2-hedron.
- In the context of quantum information, the problem of constructing SIC POVMs was firstly tackled by Zauner[a] and popularized in 2003 through a paper by Renes et. al.[b]. The main emphasis of both Zauner and Renes et. al. lay on so-called *group covariant* POVMs.
- Covariant SIC POVM's are generated by the action of the Heisenberg-Weyl or generalised Pauli group.
- The action of this group on a seed state (**fiducial state**) generates d^2 equidistant states).
- They seem to exist in all dimensions, although there are only numerical results that support this conjecture. This is because in general the analytical expression of those states is unknown but there exist very accurate numerical estimations of their amplitudes.

[a] G. Zauner Quantumdesigns: Grundzuge einer nichtkommutativen Designtheorie Ph.D. thesis (Univ Wien) (1999).

[b] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, J. Math. Phys. 45, 2171 (2004), Symmetric Informationally Complete Quantum Measurements.

SICs and Clifford transformations.

- An important property of SICs is that if we know one fiducial state of a particular covariant SIC we can generate many other covariant SICs by transforming this fiducial state under the elements of the Clifford group.
- The Clifford group is the subset of the unitary operators that map Weyl operators to multiples of Weyl operators under conjugation[a]

$$Cw(q,p)C^{\dagger} = c(q,p)w(S(q,p)) \tag{20}$$

for maps $c : \mathbb{Z}_d^2 \to \mathbb{C}$ and $S : \mathbb{Z}_d^2 \to \mathbb{Z}_d^2$.

- Among other properties the map S is invertible and $S(0,0) = (0,0)$; the operation associated to its invert S^{-1} is $C^{\dagger}$.

[a] In prime dimensions the Clifford transformations are nothing else than the unitaries mapping one MUB onto another MUB. The Hadamard transformation is a qubit Clifford operator for instance. In prime power dimensions one can define a generalized Clifford group along these lines. The matrix S preserves then the symplectic product.

SICs and Clifford transformations.

- From the definition, it is straightforward to check that the image of the fiducial state of a SIC under a Clifford transformation is still a SIC fiducial state.
- **Proof**
- The proof goes as follows; let us assume that the state $|U_{0,0}\rangle$ is a fiducial state so that $|\,\mathrm{tr}\,|U_{0,0}\rangle\langle U_{0,0}|w(m,n)| = |\langle U_{0,0}|w(m,n)|U_{0,0}\rangle|$ $=\sqrt{1/(d+1)}$ whenever $m \neq 0$ or $n \neq 0$;
- then its image $|U'_{0,0}\rangle$ under a Clifford transformation $C^\dagger$ satisfies

  $|\,\mathrm{tr}\,|U'_{0,0}\rangle\langle U'_{0,0}|w(m,n)| = |\langle U_{0,0}|Cw(m,n)C^\dagger|U_{0,0}\rangle|$
  $=|\,\mathrm{tr}\langle U_{0,0}|w(S(m,n))|U_{0,0}\rangle|$
  $=|\,\mathrm{tr}\langle U_{0,0}|w(m',n')|U_{0,0}\rangle|$
  $=\sqrt{1/(d+1)}$

  where we made use of the fact that the map S is invertible and $S(0,0) = (0,0)$ so that if $m \neq 0$ or $n \neq 0$ then $m' \neq 0$ or $n' \neq 0$.

SICs and Clifford transformations.

- Consequently, if we know a fiducial state of a particular H-W covariant SIC, then we can generate a set of other fiducial states and SICs by letting act on it the Clifford transformations. As these operations form a group, such sets are classes of equivalence of fiducial states (orbits under the Clifford group).

  Two remarkable properties characterize these orbits:

  -The number of orbits is very low (one or two).

  Example: in dimension 6 there are 3456 fiducial states: 1728 of them belong to the same orbit, and the 1728 other fiducial states are their images by complex conjugation.

  -The second property is the so-called

Zauner's conjecture.

-It seems that there always (in arbitrary dimension d) exists a fiducial state that is eigenvector under a certain Clifford operation[a].

[a] Actually this operation generates a subgroup of the Clifford group of order 3; as a consequence the number of fiducial states is equal to the number of Clifford transformations divided by 3 times an integer.

SICs and Clifford transformations.

- The validity of Zauner's conjecture has been checked for all dimensions up to 141, as well as 143,147,168,172,195,199,228,259,323 and 844[a] by a bunch of authors (Scott, Grassl, Appleby, Fuchs and so on)[a], most often with a 15 digit accuracy but exact solutions are also known for instance for dimensions 2-24,28,30,31,35,37,39,43,48,124.
- Recently, I. Bengtsson found[b], using similar numerical techniques, the existence of a fiducial state for a H-W covariant SIC POVM in dimension $d = 5779$...
- Due to applications in code theory, dimension 2048 deserves to be patented according to certain "rumors"[a].

[a] Fuchs, C.A.; Hoang, M.C.; Stacey, B.C. The SIC Question: History and State of Play. Axioms 2017, 6, 21.

[b] Private communication.

QUBIT SIC POVMs.

- qubit POVM is sufficient for tomography whenever the 4 collected probabilities are independent (up to normalization); then we get 3 independent parameters equivalent to Bloch (spin 1/2) or Stokes (polarisation of light) parameters up to reparametrization. Such a POVM is called IC (Informationally Complete) POVM.

- Optimal POVM tomography corresponds to the situation where the 4 states $|U^S_{k,j}\rangle$ are treated on the same footing and maximally independent.

- In the qubit case this occurs when they form a perfect tetrahedron on the Bloch sphere.

- Qubit SIC (Symmetric Informationally Complete) POVMs are thus associated to a tetrahedron on the Bloch sphere.

Example 1: SIC POVM of. spin 1/2 particles in NMR systems.

- We wish to estimate the Bloch parameters k_x, k_y, and k_z necessary in order to describe the unknown state of the qubit a.
- An ancilla is added to this device as qubit b to form a extending system. This device is initially prepared in the state: $\rho_{in} = \rho_a \otimes |0\rangle \langle 0|_b$. This state differs according to different input qubits a.

- We let now evolve the entire system under U, a (well-chosen) unitary evolution:

$$U = \frac{1}{2}\begin{pmatrix} e^{i\pi/4}\alpha & \alpha & \beta & -e^{i\pi/4}\beta \\ \alpha & -e^{-i\pi/4}\alpha & -e^{-i\pi/4}b & -\beta \\ \beta & -e^{i\pi/4}\beta & e^{i\pi/4}\alpha & \alpha \\ -e^{-i\pi/4}\beta & -\beta & \alpha & -e^{-i\pi/4}\alpha \end{pmatrix}$$

where $\alpha = \sqrt{1+1/\sqrt{3}}, \beta = \sqrt{1-1/\sqrt{3}}$.

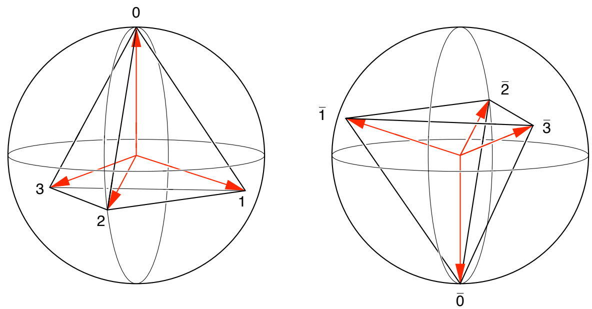
- By measuring the full system in a basis that consists of the product of the a and b qubit computational bases, we obtain four probabilities $P_{00}, P_{01}, P_{10}, P_{11}$.

- Such a POVM measurement is informationally complete due to the fact that the coefficients $P_{00}, P_{01}, P_{10}, P_{11}$ are in one-to-one correspondence with the Bloch parameters k_x, k_y, and k_z as shows the identity

$$\begin{cases} P_{00} = \frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(k_x+k_y+k_z)\right] \\ P_{01} = \frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(-k_x-k_y+k_z)\right] \\ P_{10} = \frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(k_x-k_y-k_z)\right] \\ P_{11} = \frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(-k_x+k_y-k_z)\right] \end{cases}$$

Remark 1.

- Actually, P_{00} is the average value of the operator $(\frac{1}{2})(\sigma_{0,0} + (\frac{1}{\sqrt{3}})(\sigma_{1,0} + \sigma_{0,1} + \sigma_{1,1}))$ which is the projector onto the pure state $|\phi\rangle\langle\phi|$ with $|\phi\rangle = \alpha|0\rangle + \beta^*|1\rangle$ and $\alpha = \sqrt{1 + \frac{1}{\sqrt{3}}}$, $\beta^* = e^{\frac{i\pi}{4}}\sqrt{1 - \frac{1}{\sqrt{3}}}$.
- Under the action of the Pauli group it transforms into a projector onto one of the four pure states $\sigma_{i,j}|\phi\rangle$; $i, j : 0, 1$: $\sigma_{i,j}|\phi\rangle\langle\phi|\sigma_{i,j} = (\frac{1}{2})((1 - \frac{1}{\sqrt{3}})\sigma_{0,0} + (\frac{1}{\sqrt{3}})(\sum_{k,l=0}^{1}(-)^{i.l-j.k}\sigma_{k,l}))$
- The signs $(-)^{i.l-j.k}$ reflect the (anti)commutation properties of the Pauli group. So, the four parameters P_{ij} are the average values of projectors onto four pure states that are "Pauli displaced" of each other. The in-product between them is equal, in modulus, to $1/\sqrt{3} = 1/\sqrt{d+1}$, with $d = 2$.
- This shows that this POVM is symmetric in the sense that it is in one-to-one correspondence with a tetrahedron on the Bloch sphere; this tetrahedron is obviously invariant under the action of the Pauli group, so it is an example of H-W cocariant SIC POVM...



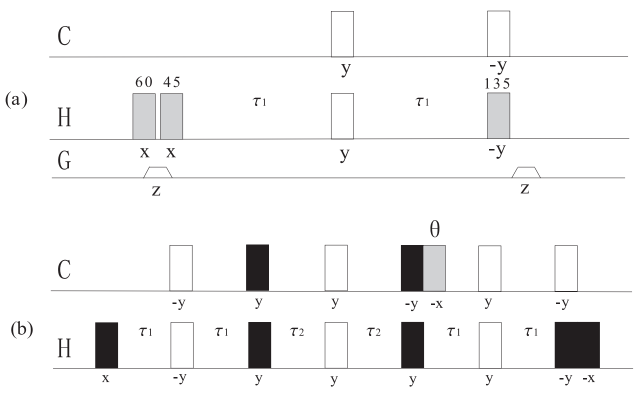
Tetrahedron and its complex conjugate (anti-tetrahedron).

Remark 2.

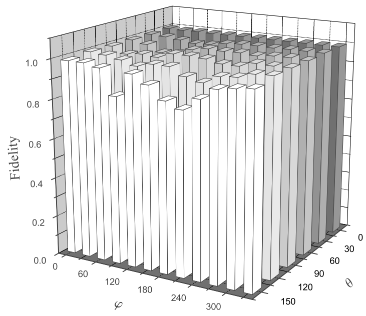
- SIC POVM tomography of a proton trapped in a chloroform molecule has been realized in China, at the Quantum Information lab. of Hefei University[a].
- The ancilla was another proton, neighbour to the first one.
- Their unitary evolution was a judicious combination of external Radio-Frequency Pulses (local qubit rotations) and of non-local (entangling) Ising spin-spin (neighbour-neighbour) interaction.

[a] JF Du, M. Sun, X. Peng and T. Durt, Entanglement Assisted NMR Tomography of a Qubit, Phys. Rev. A, **74**, 042341 (2006).

NMR SIC POVM tomography of a psin 1/2 state.



NMR pulses sequence.



Fidelity for 120 different initial qubit states.

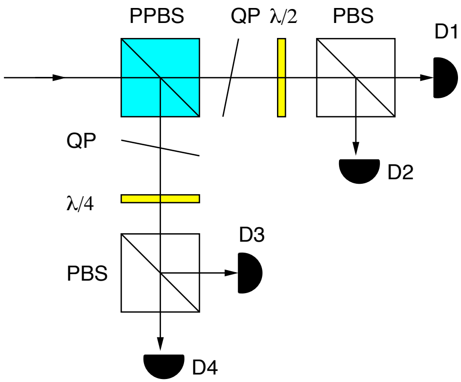
Example 2: Polarimetry by SIC POVM tomography.

- Traditionally, in order to estimate the polarisation (Stokes-Jones) parameters, three PVM measurements are necessary, in 3 different polarisation bases.
- To perform SIC POVM polarimetry, one measurement with 4 detectors is enough.
- This has been realized at Singapore University (NUS).
- To do so, the polarisation was coupled (entangled) to spatial localisation by letting pass the pulses through a partially polarising beamsplitter (PPBS) (see picture next page[a]).

[a] from the reference A. Ling, S-K Pang, A. Lammas-Linares, and C. Kurtsiefer, $Phys.Rev.A$ **74**, 022309 (2006)).

SIC POVM tomography

of photonic polarisation states.



Polarimetry set-up

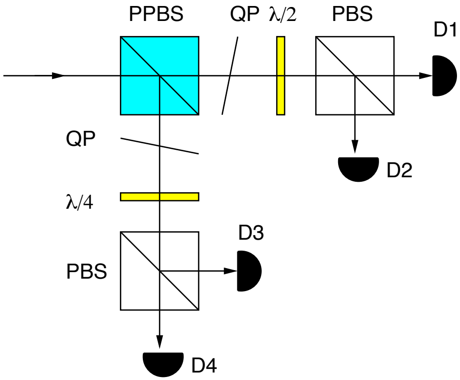
- By adjusting the asymmetry of the PPBS and the angle of the wave plates (half wave and quarter wave plates) in an ad hoc manner, the four b detectors will fire with the same P probabilities as for the spin 1/2 case: $k_y b1 = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(k_x + k_y + k_z)\right]$, $P_{b2} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(-k_x - k_y + k_z)\right]$, $P_{b3} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(k_x - k_y - k_z)\right]$, $P_{b4} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(-k_x + k_y - k_z)\right]$.

2 qubit SIC Full Tomographic Protocol for QKD.

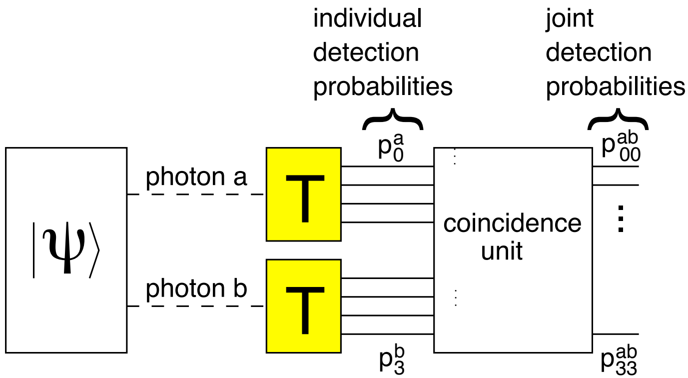
- In the so-called Singapore protocol for QKD[a], a pair of photons is prepared in a maximally entangled polarisation state (Bell state) in a non-linear crystal.
- Those photons are emitted along opposite directions to the authorized users of the cryptographic line, Alice and Bob, who measure their polarisation by a SIC POVM measurement.
- Bell states exhibit isotropic anti-correlations when they are measured by local SIC POVM devices.
- These anti-correlations are exploited by Alice and Bob in order to establish a fresh cryptographic key, which is the goal of quantum cryptographic protocols.

[a] T.Durt, C. Kurtsiefer, A. Lamas-Linares, A. Ling: Phys. Rev. A 78, 1 (2008), Wigner Tomography of two-qubit states and quantum cryptography.

2 qubit SIC Full Tomographic Protocol for QKD.



Local set-up

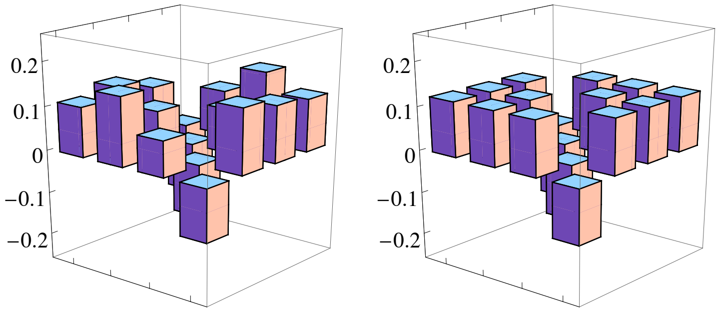


Global set-up

2 qubit SIC Full Tomographic

Wigner Tomography

of a Bell state.



Experimental versus theoretical Wigner distribution of a Singlet State.

Qutrit SIC POVMs.

- For qutrits an interesting fiducial state can be found for which SIC POVM tomography is equivalent to Wigner tomography[a].
- It is the unique eigenstate of the Parity operator (proportional to $\hat{W}_{00}$) for the eigenvalue -1.
- Let us denote this state $|\Psi_- >$:
  $(1/2)(\hat{\mathbb{1}} - P\hat{a}r.) = |\Psi_- >< \Psi_-|$
- The Wigner operators and the projectors onto elements of the elements of the HW covariant equiangular set are related by a linear relation of the type $\hat{W}_{ij} = a\hat{\mathbb{1}} + b\hat{U}_{ij}|\Psi_- >< \Psi_-|\hat{U}_{ij}^{\dagger}$ with a and b real parameters.
- A similar relation also holds in the qubit case where each state of the tetrahedron is eigenstate of a Wigner operator.
- A simple dimensional argument explains[a] why it is only in dimensions 2 and 3 that such a relation is valid.

[a] S. Colin, J. Corbett, T. Durt and D. Gross: "About SIC POVMs and discrete Wigner distribution", J. Opt. B: Quantum Semiclass. Opt. 7 S778-S785 (2005))

Conclusion.

- This is where we end this visit in the zoo of applications of the H-W group to tomography.
- We mentioned their interest for cryptography, but they are also relevant in quantum computing, code theory, and signal-processing tasks like radar and speech recognition[a].
- They provide a picture of phase-space that goes far beyond its classical description[b].

[a] Fuchs, C.A.; Hoang, M.C.; Stacey, B.C.: Axioms (2017), 6, 21, The SIC Question: History and State of Play. .

[b] T. Durt, B-G Englert, I. Bengtsson, and K. Zyczkowski: IJQI, vol. 8, nr 4, 535-640 (2010), On mutually unbiased bases.