Coherent states of the p-adic Heisenberg group, heterodyne measurements and entropic uncertainty relations

Evgeny Zelenov

Steklov Mathematical Institute
New Trends in Mathematical Physics
November 7 – 12, 2022

- Coherent states
- A little about p-adic
- Heisenberg group and CCR
- A little more about p-adic
- Coherent states
- Husimi function, Wehrl entropy
- Heterodyne measurement and some entropic inequalities
- Entropic uncertainty relations
- Mutually unbiased bases

Let G be a locally compact group and $U(g)$, $g \in G$ its irreducible unitary representation in a separable complex Hilbert space $\mathcal{H}$.
Fix a unit vector $|\psi\rangle \in \mathcal{H}$ and consider the subgroup $H \subset G$ with the property:

$$U(h)|\psi\rangle = e^{i\omega(h)}|\psi\rangle,\ h \in H.$$

Let $X = G/H$ and $g(x)$ be an arbitrary representative from a coset $x \in X$. The following set:

$$\{|x\rangle = U(g(x))|\psi\rangle,\ x \in X\}$$

is the system of (generalized) coherent states[1]. It is easy to see that $|x\rangle\langle x|$ does not depend on the choice of a representative $g(x)$ from coset x.
If we apply the procedure to the Heisenberg group and vacuum vector as $|\psi\rangle$ then we obtain the well-known coherent states in quantum theory.

---

[1] A. M. Perelomov. Coherent states for arbitrary Lie group, Commun. Math. Phys, **26**, 222-236 (1972)

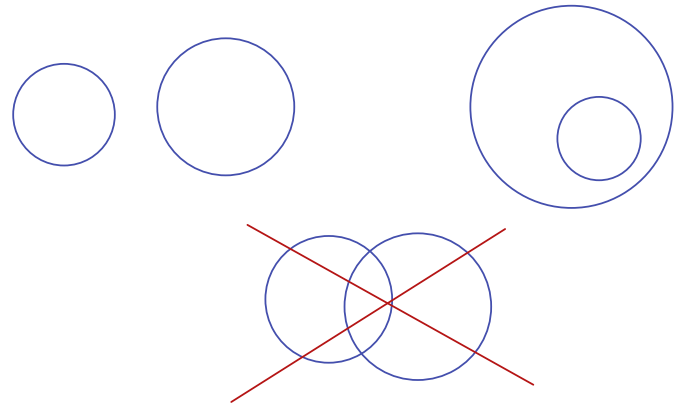
We fix a prime number p. Any rational number $x \in \mathbb{Q}$ is uniquely representable as

$$x = p^k \frac{m}{n},\ k, m, n \in \mathbb{Z},\ p \nmid m,\ p \nmid n.$$

Let's define the norm $|\cdot|_p$ on $\mathbb{Q}$ by the formula $|x|_p = p^{-k}$,
Completion of the field of rational numbers with this norm is the field $\mathbb{Q}_p$ of p-adic numbers.The p-adic norm of a rational integer $n \in \mathbb{Z}$ is always less than or equal to one, $|n|_p \leq 1$, the completion of rational integers $\mathbb{Z}$ with the p-adic norm is denoted by $\mathbb{Z}_p$.
$\mathbb{Z}_p = x \in \mathbb{Q}_p : |x|_p \leq 1$, that is, it is a disk of a unit radius.
For the p-adic norm, the strong triangle inequality holds:

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}.$$

The non-Archimedean norm defines totally disconnected topology on $\mathbb{Q}_p$ (the disks are open and closed simultaneously).
Two disks either do not intersect, or one lies in the other.



Locally constant functions are continuous, for example:

$$h_{\mathbb{Z}_p}(x) = \begin{cases} 1, x \in \mathbb{Z}_p \\ 0, x \notin \mathbb{Z}_p \end{cases}$$

is a continuous function.
$\mathbb{Q}_p$ is Borel isomorphic to the real line $\mathbb{R}$. The shift-invariant measure dx by $\mathbb{Q}_p$ is normalized in such a way that $\int_{\mathbb{Z}_p} dx = 1$.

For any nonzero p-adic number, the canonical representation holds:

$$\mathbb{Q}_p \ni x = \sum_{k=-n}^{+\infty} x_k p^k,\ n \in \mathbb{Z}_+,\ x_k \in \{0, 1, \ldots, p-1\}$$

$$\underbrace{p^{-n}x_{-n} + p^{-n+1}x_{-n+1} + \cdots + p^{-1}x_{-1}}_{\{x\}_p} + \underbrace{x_0 + px_1 + \cdots + p^k x_k + \cdots}_{[x]_p}$$

The following function, which takes values in a unit circle $\mathbb{T}$ in $\mathbb{C}$, is the additive character of the field of p-adic numbers.

$$\chi_p(x) = \exp\left(2\pi i \{x\}_p\right),\ \chi_p(x+y) = \chi_p(x)\chi_p(y)$$

p-Adic integers $\mathbb{Z}_p$ form a group with respect to addition (a consequence of the non-Archimedean norm) and it is profinite (procyclic) group. This is the inverse limit of finite cyclic groups $\mathbb{Z}/p^n\mathbb{Z}$, $n \in \mathbb{N}$.

$$\mathbb{Z}/p\mathbb{Z} \longleftarrow \cdots \longleftarrow \mathbb{Z}/p^n\mathbb{Z} \longleftarrow \mathbb{Z}/p^{n+1}\mathbb{Z} \longleftarrow \cdots$$

Consider the group $\hat{\mathbb{Z}}_p$ of characters $\mathbb{Z}_p$. This group has the form

$$\hat{\mathbb{Z}}_p = \mathbb{Q}_p \,/\, \mathbb{Z}_p = \mathbb{Z}(p^\infty) = \{\exp(2\pi i m/p^n),\ m, n \in \mathbb{N}\}\,.$$

This is the Prüfer group. It is a direct limit of finite cyclic groups (i.e. quasicyclic) of order p^n.

$$\mathbb{Z}/p\mathbb{Z}_p \to \mathbb{Z}/p^2\mathbb{Z}_p \to \cdots \to \mathbb{Z}/p^n\mathbb{Z}_p \to \cdots$$

Let $V = \mathbb{Q}_p^2$ be a two-dimensional vector space over $\mathbb{Q}_p$ and Δ be a non-degenerate symplectic form on this space. On the set $V \times \mathbb{Q}_p$, we define a group operation according to the rule:

$$(u, s)(v, t) = (u + v, s + t + \Delta(u, v)),\ u, v \in V,\ s, t \in \mathbb{Q}_p\,.$$

The set $V \times \mathbb{Q}_p$ equipped with such an operation is the p-adic Heisenberg group $Heis(\mathbb{Q}_p)$. The set of elements $\{(0, s),\ s \in \mathbb{Q}_p\}$ forms a commutative subgroup Z (center) of the Heisenberg group. Now let's apply Perelomov's construction to the groups $Heis(\mathbb{Q}_p)$ and Z as the group G and its subgroup H respectively.
More familiar (completely equivalent) is the language of representations of canonical commutation relations (or Weyl systems).
Let $\mathcal{H}$ be a separable complex Hilbert space. A map from V to a set of unitary operators on $\mathcal{H}$ satisfying the condition

$$W(u)W(v) = \chi_p(\Delta(u, v))W(v)W(u),\ u, v \in V$$

is called a representation of canonical commutation relations (CCR). We will also require continuity in a strong operator topology and irreducibility. When these conditions are met, such a representation is unique up to unitary equivalence.
Let's choose an arbitrary unit vector $|\psi\rangle \in \mathcal{H}$. The set of vectors in $\mathcal{H}$ of the form

$$\{|z\rangle = W(x)|\psi\rangle,\ z \in V\}$$

is called a system of (generalized) coherent states.
The next element of the construction is the choice of the vector $|\psi\rangle$. The Heisenberg group over the field of real numbers is a Lie group. The standard approach is the transition to the corresponding Lie algebra. The vacuum vector is defined as the eigenvector of the annihilation operator. In the p-adic case, there is no structure of a smooth manifold on the Heisenberg group and, accordingly, there is no corresponding Lie algebra. We will use a different approach to the construction of the vacuum vector.

p-Adic integers $\mathbb{Z}_p$ form a ring. Let L be a two-dimensional $\mathbb{Z}_p$-submodule of the space V. Such submodules will be called lattices.
On the set of lattices, we introduce the operations $\vee$ and $\wedge$:

$$L_1 \vee L_2 = L_1 + L_2 = \{z_1 + z_2,\, z_1 \in L_1,\, z_2 \in L_2\},$$

$$L_1 \wedge L_2 = L_1 \cap L_2.$$

We also define the involution $*$:

$$L^* = \{z \in V : \Delta(z, u) \in \mathbb{Z}_p \, \forall u \in L\}.$$

It's easy to see that $(L_1 \wedge L_2)^* = L_1 \vee L_2$. The lattice L invariant with respect to the involution is called self-dual, $L = L^*$.
We normalize the measure on V in such a way that the volume of a self-dual lattice is equal to one. Symplectic group
$Sp(V) = SL_2(\mathbb{Q}_p)$ acts transitively on the set of self-dual lattices (and preserves the measure).

By $\mathcal{L}$ we denote the set of self-dual lattices. On the set $\mathcal{L}$, we define metric d by the formula

$$d(L_1, L_2) = \frac{1}{2} \log \#\left(L_1 \vee L_2 / L_1 \wedge L_2\right)$$

log everywhere further denotes the logarithm to the base p, $\#$ is the number of elements of the set.

Example

Let $\{e, f\}$ be a symplectic basis in V, $\Delta(e, f) = 1$.Then the lattices

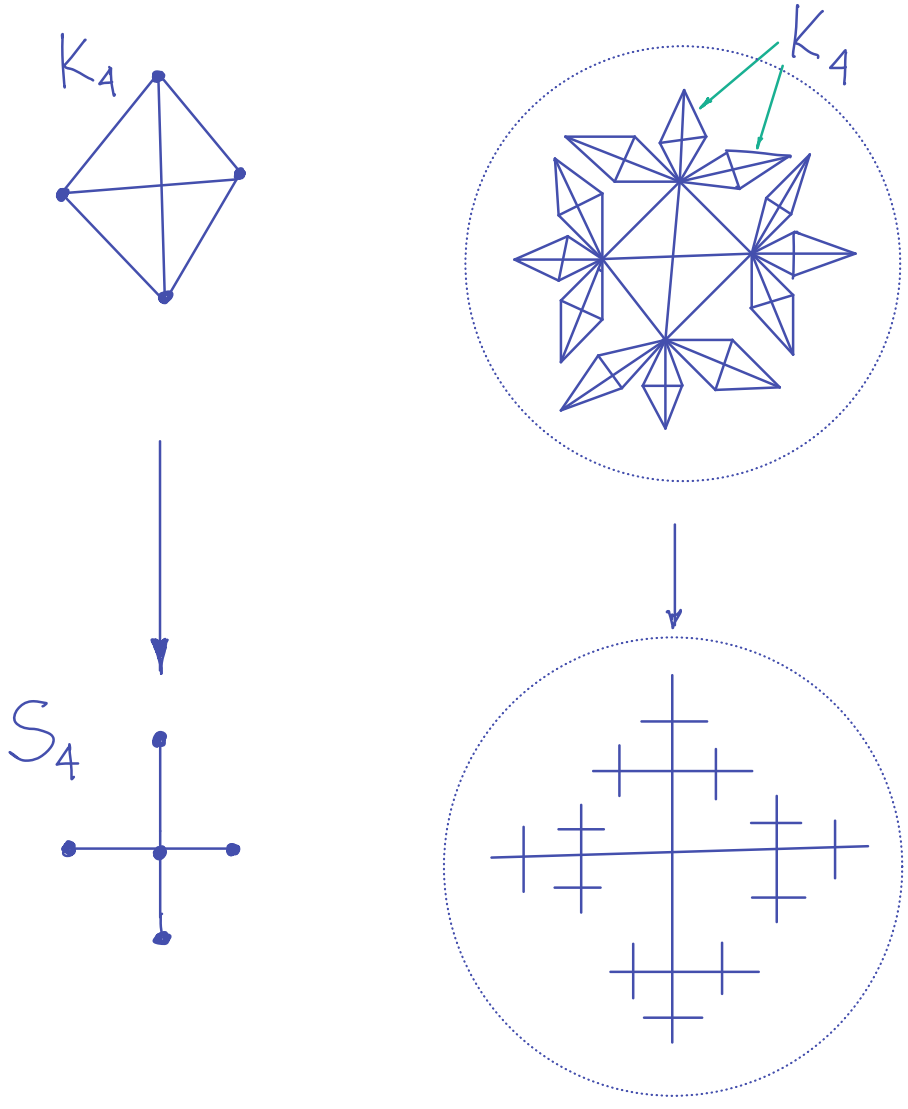
$$L_1 = \mathbb{Z}_p\, e \oplus \mathbb{Z}_p\, f, \;\; L_2 = p^n\, \mathbb{Z}_p\, e \oplus p^{-n}\, \mathbb{Z}_p\, f$$

are self-dual. If $n \geq 0$, then

$$L_1 \wedge L_2 = p^n\, \mathbb{Z}_p\, e \oplus \mathbb{Z}_p\, f, \;\; L_1 \vee L_2 = \mathbb{Z}_p\, e \oplus p^{-n}\, \mathbb{Z}_p\, f$$

$$d(L_1, L_2) = \frac{1}{2} \log \#\left(L_1 \vee L_2 / L_1 \wedge L_2\right) = \frac{1}{2} \log p^{2n} = n$$

Note that for any pair of self-dual lattices, such a basis exists.
The set of self-dual lattices can be represented as a graph. The distance d takes values in the set of non-negative integers. The vertices of the graph are elements of the set $\mathcal{L}$, and the edges are pairs of self-dual lattices $\{L_2, L_2\}$: $d(L_1, L_2) = 1$.
The graph of self-dual lattices is constructed according to the following rule. Let K_{p+1} denote a complete graph with $p + 1$ vertices.The countable family of copies of the graph K_{p+1} is glued together in such a way that each vertex of each graph in this family belongs to exactly $p + 1$ graphs K_{p+1}.
By replacement of each complete graph K_{p+1} by a star graph S_{p+1} we get a Bruhat-Tits tree.
Below is a picture for $p = 3$.


K_4
K_4
S_4

We proceed with the construction of the vacuum vector. Let us choose a self-dual lattice $L \in \mathcal{L}$ and consider the operator

$$P_L = \int_L dz W(z).$$

Lemma

The P_L operator is a one-dimensional projection.

$$P_L^2 = \int_L dz W(z) \int_L dz' W(z') =$$

$$= \int_I dz \int_L dz' W(z+z') = \int_L dz W(z) = P_L$$

The one-dimensionality of the projection P_L directly follows from the irreducibility of the representation W.
Our desired vacuum state will be this projection. We fix the notation $P_L = |0_L\rangle\langle 0_L|$.

Definition

The family of vectors $\{|z_L\rangle = W(z)|0_L\rangle,\ z \in V\}$ in $\mathcal{H}$ is said to be the system of (L-)coherent states.

We denote by h_L the indicator function of the lattice L,

$$h_L(z) = \begin{cases} 1, z \in L \\ 0, z \notin L \end{cases}$$

Theorem

Coherent states satisfy the following relation:

$$|\langle z_L|z'_L\rangle| = h_L(z - z').$$

In other words, the coherent states $|z_L\rangle\langle z_L|$ and $|z'_L\rangle\langle z'_L|$ coincide if $z - z' \in L$ and are orthogonal otherwise.

Indeed, let $u = z - z'$. Then

$$|\langle z_L|z'_L\rangle| = |\chi_p(1/2\Delta(z,u))\langle 0_L|W(u)0_L\rangle = |\langle 0_L|W(u)0_L\rangle|.$$

If $u \in L$ the statement of the theorem follows from the definition of a vacuum vector. If $u \notin L$, then by virtue of the self-duality of the lattice L, there exists $v \in L$ that $\chi_p(\Delta(u,v)) \neq 1$. We have

$$\langle 0_L|W(u)0_L\rangle = \langle 0_L|W(-v)W(u)W(v)0_L\rangle = \\ = \chi_p(\Delta(u,v))\langle 0_L|W(u)0_L\rangle,$$

which is true only if $\langle 0_L|W(u)0_L\rangle = 0$.
Therefore, non-matching (and pairwise orthogonal) coherent states are parametrized by elements of the set
$V/L = (\mathbb{Q}_p/\mathbb{Z}_p)^2 \cong \mathbb{Z}(p^\infty) \times \mathbb{Z}(p^\infty)$. This makes the following definition natural.

Definition

The set $\{|\alpha_L\rangle = W(\alpha)|0_L\rangle,\ \alpha \in V/L\}$ is said to be the set of coherent states for the p-adic Heisenberg group.

Let ρ be a density matrix, that is, ρ is a positive operator with a unit trace in $\mathcal{H}$.
We will be interested in the following objects:

- Husimi function $Q^L_\rho(z) = \langle z|\rho|z'\rangle$,
- Werhl entropy $S^L_W(\rho) = -\int_V Q^L_\rho(z) \log Q^L_\rho(z) dz$.

Proposition

The Husimi function is constant on adjacency classes V/L and is thus defined on the set V/L.
For the Wehrl entropy the following equality is valid.

$$S^L_W(\rho) = -\sum_{\alpha \in V/L} Q^L_\rho(\alpha) \log Q^L_\rho(\alpha)$$

Both statements are obvious consequences of the orthogonality Theorem for coherent states.

Proposition

The Husimi function defines the probability distribution on the set V/L, that is

$$Q_\rho^L(\alpha) \geq 0, \quad \sum_{\alpha \in V/L} Q_\rho^L(\alpha) = 1.$$

The following map

$$\rho \to \rho_{out} = \Phi_L[\rho] = \sum_{\alpha \in V/L} Q_\rho^L(\alpha) |\alpha_L\rangle\langle\alpha_L|$$

defines the quantum-classical channel Φ_L.
This is a complete ideal quantum measurement associated with an orthonormal basis of p-adic coherent states.
This measurement is heterodyne, that is, the coordinate and momentum of the particle are measured simultaneously with the maximum accuracy allowed by the uncertainty relation.
Denote by $S(\rho) = -\operatorname{Tr} \rho \log \rho$ the von Neumann entropy.
The Wehrl entropy has the following properties.

- $S(\rho) \leq S_W^L(\rho)$.
  This property also holds in the case of the real (i.e. over $\mathbb{R}$) Heisenberg group.
- $S_W^L(\rho) = S\left(\Phi_L[\rho]\right)$.
  In other words, the Wehrl entropy of a state ρ is the von Neumann entropy of the measurement result in the basis of coherent states. This is a consequence of the orthogonality of p-adic coherent states and does not hold in the real case.
  In the real case, there is an estimate of $S_W(\rho) \leq S(\rho_{out})$ (Berezin-Lieb inequality[2]).
- $0 \leq S_W^L(\rho)$, $S_W^L(\rho) = 0$ if and only if ρ is a coherent state.
  In the real case, the inequality $1 \leq S_W(\rho)$ is valid and equality occurs only on coherent states (the Wehrl-Lieb inequality).[3] [4]
  This is a non-trivial result.
  In the p-adic case, this is a very simple statement, which directly follows from a simple observation that the Husimi

function of a coherent state takes only two values – zero and one,

$$Q^{L}_{|\beta_L\rangle\langle\beta_L|}(\alpha) = \delta_{\alpha\beta}.$$

[2] F./,A./Berezin. The general concept of quantization. Commun. Math, Phys. **40**, 153 (1975)

[3] A. Wehrl. On the relation between classical and quantum-mechanical entropy. Reports on Math. physics, **16**, 3, 353-358 1979.

[4] E. H. Lieb. Proof of an entropy conjecture of Wehrl. Commun. Math. Phys. 62, 35-41 (1978)

The channel Φ_L looks very simple in the representation of characteristic functions. The characteristic function π_ρ of the quantum state ρ is given by the relation

$$\pi_\rho(z) = \mathrm{Tr}\, \rho W(z),\ z \in V$$

and defines the state uniquely.

Proposition

The channel Φ_L multiplies the characteristic function of the state by the indicator function of the lattice L:

$$\pi_{\Phi_L[\rho]}(z) = \pi_\rho(z) h_L(z),\ z \in V.$$

Now let two self-dual lattices L_1 and L_2 be given. These lattices are corresponded to measurements in the bases of coherent states.

From the previous sentence, it's easy to see what sequential measurements look like. Namely:

$$\pi_\rho \xrightarrow{\Phi_{L_1}} \pi_\rho h_{L_1} \xrightarrow{\Phi_{L_2}} \pi_\rho h_{L_1} h_{L_2} = \pi_\rho h_{L_2} h_{L_1} = \pi_\rho h_{L_1 \wedge L_2}$$

The composition of channels is thus naturally denoted by $\Phi_{L_1 \wedge L_2}[\rho]$.

Proposition

The channel $\Phi_{L_1 \wedge L_2}$ is an incomplete ideal measurement. The orthogonal decomposition of the unit corresponding to this measurement is $\{P_a,\ a \in V/L_1 \vee L_2\}$. All projections P_a have the same dimension equal to $d(L_1, L_2)$.

The entropy of the output state for the channel $\Phi_{L_1 \wedge L_2}[\rho]$ is denoted by $S_W^{L_1 \wedge L_2}$.

Proposition

The entropy $S_W^{L_1 \wedge L_2}$ satisfies the inequality $d(L_1, L_2) \leq S_W^{L_1 \wedge L_2}(\rho)$. The bound is optimal, equality occurs for L_1- or L_2-coherent states.

Theorem

The following inequalities are valid:

$$S_W^{L_1 \wedge L_2}(\rho) \leq S_W^{L_1}(\rho) + S_W^{L_2}(\rho) \leq 2 S_W^{L_1 \wedge L_2}(\rho)$$

The lower bound occurs for L_1- or L_2-coherent states, the upper bound occurs for a maximally chaotic state in the subspace spanned by coherent states $|\alpha_{L_1}\rangle \in (L_1 \vee L_2)/L_1$.

The entropic uncertainty relation follows directly from the last two statements.

Corollary

The inequality (entropic uncertainty relation) is valid.

$$d(L_1, L_2) \leq S_W^{L_1}(\rho) + S_W^{L_2}(\rho).$$

Equality occurs for L_1- or L_2-coherent states.

Such an uncertainty relations for measurements in orthogonal bases have been considered in many papers.[56]

Applying the results of Lieb and Frank[7] we can get a stronger estimate:

$$d(L_1, L_2) + S(\rho) \leq S_W^{L_1}(\rho) + S_W^{L_2}(\rho).$$

Equality is also occurs for L_1- or L_2-coherent states (these states are pure and the von Neumann entropy is zero on them).

---

[5] H. Maassen, J.B.M. Uffink: Generalized entropic uncertainty relations: Phys. Rev. Lett. 60, 1103–1106 (1988)

[6] K. Kraus. Complementary observables and uncertainty relations. Phys. Rev. D, bf 35, 10, 3070-3075 (1987)

[7] R. L. Frank, E. H. Lieb. Entropy and uncertainty principle. Ann. Henri Poincare 13, 1711-1717 (2012)

Mutually unbiased bases in Hilbert space $\mathbb{C}^D$ are two orthonormal bases $\{|e_1\rangle, \ldots, |e_D\rangle\}$ and $\{|f_1\rangle, \ldots, |f_D\rangle\}$ such that the square of the magnitude of the inner product between any basis states $|e_j\rangle$ and $|f_k\rangle$ equals the inverse of the dimension D

$$|\langle e_j|f_k\rangle|^2 = \frac{1}{D}, \quad \forall j, k \in \{1, \ldots, D\}.$$

Such bases have numerous applications in quantum information theory (quantum key distribution, quantum state reconstruction, quantum error correction codes, detection of quantum entanglement, etc).
Denote by $\mathfrak{M}(D)$ the number of MUB in $\mathbb{C}^D$. In general, to find $\mathfrak{M}(D)$ is a very difficult task, for example, $\mathfrak{M}(6)$ has not been found to date, despite considerable efforts. The answer is known when the dimension D is the power of a prime number, namely $\mathfrak{M}(p^n) = p^n + 1$.

Let L_1 and L_2 be a pair of self-dual lattices, $d(L_1, L_2) \geq 1$.
It turns out that the corresponding bases of L_1- and L_2-coherent states are mutually unbiased on finite-dimensional subspaces of dimension $p^{d(L_1,L_2)}$.

Theorem

For bases of L_1- and L_2-coherent states $\{|\alpha_{L_1}\rangle,\ \alpha \in V/L_1\}$ and $\{|\beta_{L_2}\rangle,\ \beta \in V/L_2\}$ the following formula is valid

$$|\langle \alpha_{L_1} | \beta_{L_2} \rangle|^2 = p^{-d(L_1,L_2)} h_{L_1 \vee L_2}(\alpha - \beta).$$

The theorem means the following. Our Hilbert space of representation of CCR $\mathcal{H}$ decomposes into an orthogonal direct sum of finite-dimensional subspaces of the same dimension $p^{d(L_1,L_2)}$:

$$\mathcal{H} = \bigoplus_{a \in V/(L_1 \vee L_2)} \mathcal{H}_a,\ \dim \mathcal{H}_a = p^{d(L_1,L_2)}$$

In each of these subspaces, the subbasis of L_1- and L_2-coherent states are mutually unbiased.

In the case of $d(L_1, L_2) = 1$ the subspaces $\mathcal{H}_a$, $a \in V/(L_1 \vee L_2)$ have dimension p. As it can be seen from the construction of the graph of lattices, there are exactly $p + 1$ pieces of self-dual lattices with unit pairwise distances (the complete graph K_{p+1}). These lattices define a complete set of MUB in each subspace $\mathcal{H}_a$.

Remark

Instead of the field $\mathbb{Q}_p$, we can consider its algebraic extension of degree n. Such extensions exist for any n. In this case, the elementary building block of the lattice graph will be the complete graph K_{p^n+1}, which has $p^n + 1$ vertex. The coherent state bases corresponding to the vertices of this graph form a complete set of mutually unbiased bases in p^n-dimensional space.