On geometry of p-adic coherent states and mutually unbiased bases

Evgeny Zelenov

International conference
dedicated to the 100th anniversary of the birthday of V.S. Vladimirov
(Vladimirov-100)
January 9–14, 2023
Steklov Mathematical Institute, Moscow

Mutually unbiased bases[1] 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:

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

The problem is to describe the MUBs set for an arbitrary D.
Within this general statement of the problem, there is a large range of subtasks.
Denote by $\mathfrak{M}(D)$ the maximum number of MUBs in $\mathbb{C}^D$.
The first problem is **what is $\mathfrak{M}(D)$ equal to**.
It is not difficult enough to get the following estimation:

$$p_1^{n_1} + 1 \le \mathfrak{M}(D) \le D + 1,$$

where $D = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, $p_1^{n_1} < p_2^{n_2} < \cdots < p_k^{n_k}$ is prime numbers decomposition of D.

[1] J. Schwinger, Unitary operator bases. Proc. Nat. Acadm Sci. USA **46**, 570-579 (1960)

It is also known that $\mathfrak{M}(p^m) = p^m + 1$, for any prime p and $m \in \mathbb{N}$. The amazing thing is that this is almost all that is known by now. The problem of finding $\mathfrak{M}(D)$ is closely related to the well-known **Winnie-the-Pooh conjecture.**[2]
Let us consider the Lie algebra $\mathfrak{sl}_D(\mathbb{C})$ of $D \times D$ matrices with zero trace. The problem of decomposition of this algebra into a direct sum of Cartan subalgebras pairwise orthogonal with respect to the Killing form is posed.

The conjecture is as follows: $\mathfrak{sl}_D(\mathbb{C})$ is orthogonally decomposable if and only if $D = p^n$ for some prime p.

The corresponding conjecture for MUB looks like this: A complete collection of MUBs exists only in prime power dimension D.[3]

---

[2] A. I. Kostrikin, I. A. Kostrikin, and V. A. Ufnarovskii, Orthogonal decompositions of simple Lie algebras (type An), Proc. Steklov Inst. Math. 1983 (4), 113

[3] P.O. Boykin, M. Sitharam, P.H. Tiep, P. Wocjan, Mutually unbiased bases and orthogonal decompositions of Lie algebras, Quantum Information and Computation, **7**, 4, 371-382 (2007)

What does Winnie-the-Pooh have to do with it?

In the classification of simple Lie algebras , the following notations are accepted: $A_n = \mathfrak{sl}_{n+1}$.

The mumbler of the Minnie-the-Pooh «Noise in the head» (B. Zahoder):

> *Возьмем это самое слово А-пять.*
> *Зачем мы его произносим,*
> *Когда мы свободно могли бы сказать*
> *"А-шесть и "А-семь"и "А-восемь"?*

This corresponds exactly to our problem.

In the case of A-five $D = 6$ and nothing is known about $\mathfrak{M}(6)$, except $3 \leq \mathfrak{M}(6) \leq 7$. For A-six we have $D = 7$ (prime number), A-seven – $D = 8 = 2^3$, A-eight – $D = 9 = 3^2$, and in all these cases an ortogonal decomposition (and a complete set of MUBs) is constructed.

Let $\mathcal{B}$ be an orthonormal basis in $\mathbb{C}^D$. Let's call a matrix A complex Hadamard if $\mathcal{B}$ and $A(\mathcal{B})$ are mutually unbiased bases.
Two Hadamard matrices A and C are equivalent if there exist monomial matrices M_1 and M_2 such that the condition is satisfied:

$$A = M_1 C M_2.$$

The problem is to describe the sets of equivalence classes of Hadamard matrices.
There is a complete description only for the case $D \leq 5$, and for $D = 2, 3, 5$ the number of Hadamard matrices is finite, for $D = 4$ there exists a one-dinensional family. For the case $D = 6$, the existence of a complex 4-dimensional family of Hadamard matrices is proved[4], for $D = 7$, the existence of a one-dimensioin family is proved.[5]

---

[4] A. Bondal, I. Zhdanovskiy, Orthogonal pairs and mutually unbiased bases, J. Math. Sci, 216(1), 23-40 (2016)

[5] Zhdanovskiy, I.Y., Kocherova, A.S. Algebras of Projectors and Mutually Unbiased Bases in Dimension 7. J Math Sci 241, 125–157 (2019)

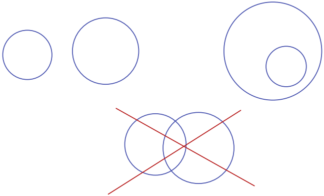
We fix a prime number p. Any rational number $x \in \mathbb{Q}$ is uniquely representable as

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

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 $\mathbb{Z}_p$.
$\mathbb{Z}_p = x \in \mathbb{Q}_p \colon |x|_p \leq 1$, 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

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

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.
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.

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 $*$:

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

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

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

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

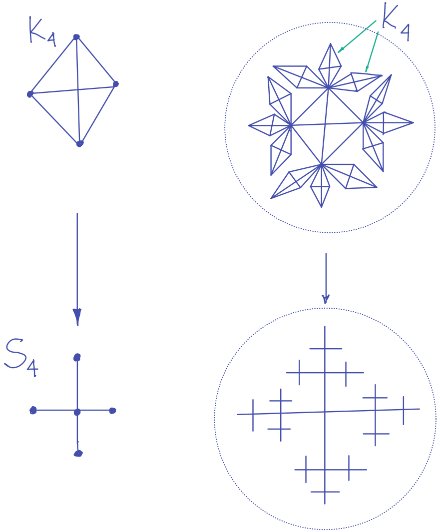
$$L_1 = \mathbb{Z}_p\, e \oplus \mathbb{Z}_p\, f\,,\ \ L_2 = p^n\, \mathbb{Z}_p\, e \oplus p^{-n}\, \mathbb{Z}_p\, f$$

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

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

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

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.

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

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 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 $\mathcal{H}_a$.

The theorem makes the following definitions natural.

Definition

Let $\mathcal{H}$ be an infinite-dimensional Hilbert space. Orthonormal bases $\{|e_i\rangle\}$ and $\{|f_j\rangle\}$ are mutually unbiased if there exists a decomposition

$$\mathcal{H} = \oplus \mathcal{H}_k, \, \dim \mathcal{H}_k = n_k < \infty,$$

such that the subbasis $\{|e_i\rangle\}|_{\mathcal{H}_k}$ and $\{|f_j\rangle\}|_{\mathcal{H}_k}$are mutually unbiased for all k.

Definition

The operator A in the Hilbert space $\mathcal{H}$ is called the Hadamard operator if for some orthonormal basis $\{|e_i\rangle\}$ in $\mathcal{H}$ the bases $\{|e_i\rangle\}$ and $A(\{|e_i\rangle\})$ are mutually unbiased.

The Hadamard operators define the dynamics of p-adic quantum system in the following sense.
Let $(W, \mathcal{H})$ be a representation of CCR and $g \in Sp(V)$. Then, by virtue of the uniqueness of the representation, the representations $(W, \mathcal{H})$ and $(W_g, \mathcal{H})$, $W_g(z) = W(gz)$, $z \in V$ are unitarily equivalent, that is, there is a unitary operator satisfying the condition

$$U(g)W(z) = W_g(z)U(g),\ z \in V.$$

Theorem

Let L be a lattice in V such that $d(L, gL) \geq 1$. Then $U(g)$ is the Hadamard operator for bases $\{|\alpha\rangle_L\}$ and $\{|\beta\rangle_{gL}\}$.