

Article

Not peer-reviewed version

# On Geometry of *p*-adic Coherent States and Mutually Unbiased Bases

Evgeny I. Zelenov \*

Posted Date: 23 May 2023

doi: 10.20944/preprints202305.1569.v1

Keywords: p-adic quantum theory; mutually; mutually unbiased bases; Hadamard matrix



Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

# On Geometry of *p*-Adic Coherent States and Mutually Unbiased Bases

## **Evgeny Zelenov**

Steklov Mathematical Institute; evgeny.zelenov@gmail.com

**Abstract:** The paper considers coherent states for the representation of Weyl commutation relations over a field of *p*-adic numbers. A geometric object, a lattice in vector space over a field of p-adic numbers, corresponds to the family of coherent states. It is proved that the bases of coherent states corresponding to different lattices are mutually unbiased, and the operators defining the quantization of symplectic dynamics are Hadamard operators.

Keywords: p-adic quantum theory mutually; mutually unbiased bases; Hadamard matrix

### 1. Introduction. MUBs.

Mutually unbiased bases (MUBs) [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  $|e_i\rangle$  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 [2–4], quantum state tomography [5], detection of quantum entanglement [6], etc).

The problem is to describe the MUBs set for an arbitrary *D*.

Within this general statement of the problem, there is a 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. 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 [7]. The answer is known when the dimension D is the power of a prime number, namely  $\mathfrak{M}(p^n) = p^n + 1$  [8].

It is possible to get the following estimation [8]:

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

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.

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 [9]. 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 [10].

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  $D \le 5$ , 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 [11], for D = 7, the existence of a one-dimension family is proved [12].

There are difficulties with definition of mutually unbiased bases in the case of an infinite-dimensional Hilbert space [13]. In this paper we will give such a definition. Despite its seeming naivety, the definition mentioned above naturally arises in the context of p-adic quantum mechanics.

I also want to note that the above brief overview and bibliographic references do not pretend to be complete, many important and interesting articles are not mentioned.

### 2. p-Adics numbers.

Just a few words about p-adic numbers, in order to introduce the necessary notation. For more information about p-adic numbers, see, for example, [14].

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

$$x = p^k \frac{m}{n}$$
,  $k, m, n \in \mathbb{Z}$ ,  $n > 0$ ,  $p \nmid m$ ,  $p \nmid n$ .

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,  $|n|_p \le 1$ , the completion of rational integers  $\mathbb Z$  with the p-adic norm is denoted by  $\mathbb Z_p$ .  $\mathbb Z_p = x \in \mathbb Q_p$ :  $|x|_p \le 1$ , that is, it is a disk of a unit radius.

For the *p*-adic norm, the strong triangle inequality holds:

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

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 on  $\mathbb{Q}_p$  (the Haar measure) is normalized in such a way that  $\int_{\mathbb{Z}_p} dx = 1$ .

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

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

Using the canonical representation, we define the integer  $[x]_p$  and fractional  $\{x\}_p$  parts of the number  $x \in \mathbb{Q}_p$ :

$$\underbrace{p^{-n}x_{-n} + p^{-n+1}x_{-n+1} + \dots + p^{-1}x_{-1}}_{\{x\}_p} + \underbrace{x_0 + px_1 + \dots + p^kx_k + \dots}_{[x]_p}.$$

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  $p^n$ :

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

# 3. Representations of CCR. Coherent states.

Let  $V = \mathbb{Q}_p^2$  be a two-dimensional vector space over  $\mathbb{Q}_p$  and  $\Delta$  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 (compact)  $\mathbb{Z}_p$ -submodule of the space V. Such submodules will be called lattices.

On the set of lattices, we introduce the operations  $\vee$  and  $\wedge$ :

$$L_1 \lor L_2 = L_1 + L_2 = \{z_1 + z_2, z_1 \in L_1, z_2 \in L_2\},$$
 
$$L_1 \land L_2 = L_1 \cap L_2.$$

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.

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 1.** 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.

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 1.** The  $P_L$  operator is a one-dimensional projection.

Indeed, we have:

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

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

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 1.** The family of states  $\{|z_L\rangle = W(z)|0_L\rangle$ ,  $z \in V\}$  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 1.** 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  $|z_I'\rangle\langle z_I'|$  coincide if  $z-z'\in L$  and are orthogonal otherwise.

Indeed, let u = z - z'. Then

$$|\langle z_L | z_I' \rangle| = |\chi_{v}(1/2\Delta(z, u)) \langle 0_L | W(u) 0_L \rangle = |\langle 0_L | W(u) 0_L \rangle|.$$

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  $\chi_v(\Delta(u,v)) \neq 1$ . We have

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

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

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 modification of Definition 1 natural.

**Definition 2.** The set  $\{|\alpha_L\rangle = W(\alpha)|0_L\rangle$ ,  $\alpha \in V/L\}$  is said to be the basis of p-adic (L-)coherent states.

**Remark 1.** The CCR representations are closely related to the representations of the Heisenberg group. In the language of representation theory, p-adic coherent states are nothing but coherent states for the p-adic Heisenberg group.

### 4. Main result.

Let  $L_1$  and  $L_2$  be a pair of self-dual lattices,  $d(L_1, L_2) \ge 1$ .

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 2.** 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 subbases of  $L_1$ - and  $L_2$ -coherent states are mutually unbiased.

Let's prove Theorem 2.

The following formula is valid.

$$|\langle 0_{L_1} | W(\beta) 0_{L_2} \rangle| = \begin{cases} |\langle 0_{L_1} | 0_{L_2} \rangle|, \beta \in L_1 \vee L_2, \\ 0, \beta \notin L_1 \vee L_2. \end{cases}$$
 (1)

Let  $\beta \in L_1 \vee L_2$ , then  $\beta = \beta_1 + \beta_2$ ,  $\beta_1 \in L_1$ ,  $\beta_2 \in L_2$  and

$$|\langle 0_{L_1}|W(\beta)0_{L_2}\rangle| = |\langle W(-\beta_1)0_{L_1}|W(\beta_2)0_{L_2}\rangle| = |\langle 0_{L_1}|0_{L_2}\rangle|.$$

If  $\beta \notin L_1 \vee L_2$ , then there exists  $\gamma \in L_1 \wedge L_2 = (L_1 \vee L_2)^*$  such that  $\chi_v (\Delta(\gamma, \beta) \neq 1$  and

$$\langle 0_{L_1}|W(\beta)0_{L_2}\rangle = \langle W(\gamma)0_{L_1}|W(\beta)W(\gamma)0_{L_2}\rangle = \chi_p\left(\Delta(\gamma,\beta)\left\langle 0_{L_1}|W(\beta)0_{L_2}\right\rangle.$$

From the latter equality, it obviously follows that  $\langle 0_{L_1}|W(\beta)0_{L_2}\rangle=0$ ,  $\beta\notin L_1\vee L_2$ .

Now let's use formula (1) and the Parseval-Steklov identity:

$$1 = \sum_{\beta \in V/L_2} \left| \langle 0_{L_1} | W(\beta) 0_{L_2} \rangle \right|^2 =$$

$$= \left| \langle 0_{L_1} | 0_{L_2} \rangle \right|^2 \sum_{\beta \in L_1 \vee L_2 / L_2} 1 = \left| \langle 0_{L_1} | 0_{L_2} \rangle \right|^2 p^{d(L_1, L_2)}. \quad (2)$$

The following equation follows from formula (2):

$$\left| \langle 0_{L_1} | 0_{L_2} \rangle \right|^2 = p^{-d(L_1, L_2)}.$$
 (3)

Taking into account formula (1) and the equality (3), we obtain a proof of Theorem 2.

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  $\mathcal{H}_a$ .

In the case of  $d(L_1, L_2) = 2$  the subspaces  $\mathcal{H}_a$ ,  $a \in V/(L_1 \vee L_2)$  have dimension  $p^2$ . As it can be seen from the construction of the graph of lattices, there are exactly p(p+1) pieces of self-dual lattices lying at a distance of 2 from the lattice  $L_1$ . The bases corresponding to these lattices are not mutually unbiased. However, among this set there are families consisting of p+1 pieces of mutually unbiased bases. These bases saturate the entropic uncertainty relations [15,16].

**Remark 2.** 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.

The theorem makes the following definitions natural.

**Definition 3.** 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 subbases  $\{|e_i\rangle\}|_{\mathcal{H}_k}$  and  $\{|f_i\rangle\}|_{\mathcal{H}_k}$  are mutually unbiased for all k.

Let's make two remarks. First, the definition assumes that the bases are divided into finite blocks of size  $n_k$ , each of which forms a subbases in the corresponding subspace  $H_k$ . Secondly, in the case under consideration of the representation of CCR over a field of p-adic numbers of the dimension of subspaces  $H_k$  there are powers of p. The construction can be extended to the case of CCR over Vilenkin groups, in which case the above dimensions can be arbitrary natural numbers.

### 5. p-Adic dynamics. Hadamard operators.

The proposed definition of mutually unbiased bases for the case of an infinite-dimensional Hilbert space makes it possible to introduce the concept of the Hadamard operator for such spaces in a similar way.

**Definition 4.** 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.

In other words, the Hadamard operator is given by an infinite block-diagonal matrix whose diagonal blocks are ordinary finite Hadamard matrices.

It turns out that the dynamics of a p-adic quantum system is determined by Hadamard operators. More detailed information about p-adic quantum theory can be found, for example, in [17,18]. The dynamics of a classical system is given by a linear symplectic transformation  $g \in Sp(V)$  of the phase space V. A one-parameter family  $g_t$  of such transformations can be specified, in which case the parameter  $t \in \mathbb{Q}_p$  is interpreted as time. For example, the dynamics of a free particle of unit mass is given by the family  $g_t$ ,  $t \in \mathbb{Q}_p$ , which in some fixed basis of space V has the form:

$$g_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$
 ,  $t \in \mathbb{Q}_p$  .

If the dynamics of a classical system is determined by the action of a symplectic group on the phase space, then the dynamics of the corresponding quantum system is given by the so-called metaplectic representation of the symplectic group in the Hilbert space of the representation of CCR. The existence of such a representation follows from the uniqueness of irreducible representations of CCR.

Let  $(W, \mathcal{H})$  be a representation (irreducible) 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

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

The operators U(g),  $g \in Sp(V)$  define a metaplectic representation of Sp(V).

**Theorem 3.** Let L be a lattice in V such that  $d(L, gL) \ge 1$ . Then U(g) is the Hadamard operator for bases  $\{|\alpha\rangle_L\}$  and  $\{|\beta\rangle_{gL}\}$ .

As mentioned above, the symplectic group acts transitively on the set of self-dual lattices. Thus, if a self-dual lattice L is given, then its image gL under the action of the symplectic transformation g is also a self-dual lattice. The validity of Theorem 3 follows from Theorem 2 for a pair of lattices L and gL.

### References

- 1. J. Schwinger, Unitary operator bases. Proc. Nat. Acadm Sci. USA 46, 570-579 (1960).
- Christopher A. Fuchs, Nicolas Gisin, Robert B. Griffiths, Chi-Sheng Niu and Asher Peres, Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy, Phys. Rev. A 56, 1163 (1997).
- 3. Dagmar Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Phys. Rev. Lett. **81**, 3018 (1998).
- 4. Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin, Security of Quantum Key Distribution Using *d*-Level Systems, Phys. Rev. Lett. **88**, 127902 (2002).
- 5. W. K. Wootters, B. D. Fields, Optimal state-determination by mutually unbiased measurements, Annals of Physics **191**, 363-381 (1989).
- Christoph Spengler, Marcus Huber, Stephen Brierley, Theodor Adaktylos, and Beatrix C. Hiesmayr, Entanglement detection via mutually unbiased bases, Phys. Rev. A 86, 022311 (2012).
- 7. P. Horodecki, L. Ridnicki and K. Zyczkowski, Five open problems in quantum information theory, PRX Quantum, 3, 010101 (2022).
- 8. A. Klappenecker and M. R" otteler, Construction of MUBs, Lect. Notes in Comp. Science 2948, 137 (2004).
- 9. A. I. Kostrikin, I. A. Kostrikin and V. A. Ufnarovskii, Orthogonal decompositions of simple Lie algebras (type  $A_n$ ), Proc. Steklov Inst. Math. 4, 113 (1983).
- 10. 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).
- 11. A. Bondal, I. Zhdanovskiy, Orthogonal pairs and mutually unbiased bases, J. Math. Sci, 216(1), 23-40 (2016).
- 12. I. Y. Zhdanovskiy, A. S. Kocherova, Algebras of Projectors and Mutually Unbiased Bases in Dimension 7. J Math Sci 241, 125–157 (2019).
- 13. Stefan Weigert and Michael Wilkinson, Mutually unbiased bases for continuous variables, Phys. Rev. A 78, 020303(R)(2008).
- 14. W. H. Schikhof, Ultrametric Calculus: An Introduction to P-Adic Analysis, Cambridge University Press, 1984.
- 15. V. Hegde and P. Mandayam, Unextendible mutually unbiased bases in prime-squared dimensions, arXiv:1508.05892 [quant-ph] (2015).
- 16. Manuel A. Ballester and Stephanie Wehner, Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases, Phys. Rev. A 75, 022319 (2007).

- 17. V. S. Vladimirov, I. V. Volovich, E. I. Zelenov, *p*-Adic analysis and mathematical physics, World Scientific, 1994.
- 18. B. Dragovich, A. Yu. Khrennikov, S. V. Kozyrev, I. V. Volovich and E. I. Zelenov, *p*-Adic mathematical physics: the first 30 years, *p*-Adic numbers, *Ultram. Anal. Appl.* **9**, 87 (2017).

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.