Representations of the p-adic rotation group towards p-adic quantum computing

Ilaria Svampa

Universität zu Köln

Algebraic and Geometric Methods of Analysis
May 25-28, 2026

Outline

p-Adic numbers

- p prime: $p = 2$ or odd
- Kurt Hensel, 1897

- Field $\mathbb{Q}_p$, with elements of the form

$$x = \sum_{n \geq n_0} x_n p^n$$

with $n_0 \in \mathbb{Z}$, $x_n \in \{0, 1, \ldots, p-1\}$
e.g. $5 \cdot 7^{-1} + 4 \cdot 7^0 + 6 \cdot 7^2 + \cdots \in \mathbb{Q}_7$

- Ring of p-adic integers $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \text{ s.t. } n_0 \geq 0\}$
e.g. $p = 1 \cdot p^1 + 0 \cdot p^2 + 0 \cdot p^3 + \cdots \in \mathbb{Z}_p$
Inverse limit $\mathbb{Z}_p \simeq \varprojlim \{\mathbb{Z}/p^k\mathbb{Z}\}_{\mathbb{N}}$

Metric completions of $\mathbb{Q}$

- Standard absolute value $|\cdot|$ on $\mathbb{Q}$
- p-Adic absolute value $|\cdot|_p$ on $\mathbb{Q}$:

$$\left|p^n \frac{r}{s}\right|_p = p^{-n} \quad \text{except} \quad |0|_p = 0$$

where $n, r, s \in \mathbb{Z}, \quad p \nmid rs$

- Strong triangle inequality $\qquad |x+y|_p \leq \max\{|x|_p, |y|_p\}$

Ostrowski's Theorem (1916)

Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to either the standard absolute value $|\cdot|$ or the p-adic absolute value $|\cdot|_p$ for a prime p.

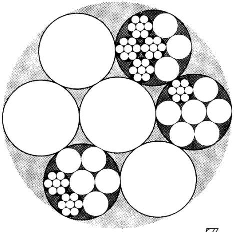
- $\mathbb{Q}_p$ is the metric completion of $\mathbb{Q}$ with respect to $|\cdot|_p$

Some properties of $\mathbb{Q}_p$

- $\mathbb{Q}_p$ is locally compact

$\mathbb{R}$ is connected

$\mathbb{Q}_p$ is totally disconnected

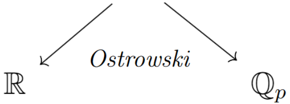


$\mathbb{Z}_7$

- $\mathbb{Q}_p$ has infinitely many closed open subgroups under addition
- $\mathbb{Q}_p$ cannot be ordered as a field
- The algebraic closure of $\mathbb{Q}_p$ has infinite degree

Motivations

- In physical observations, we deal with $\mathbb{Q}$



- *p*-Adic quantum mechanics [1]
  1. *p*-adic space
  2. symmetry group
  3. projective unitary irreducible representations (irreps)

Symmetry group of rotations on $\mathbb{Q}_p^3$
Irreps for *p*-adic angular momentum and spin
2-dimensional irreps $\leftrightarrow$ *p*-adic qubit
p-adically controlled quantum logic gates

[1] Vladimirov, Volovich, Zelenov, *p-Adic Analysis and Mathematical Physics*, 1994.

p-Adic rotation groups [2]

Unique definite quadratic form on $\mathbb{Q}_p^3$:

$$Q_+ \doteq \begin{cases} I_{3\times 3}, & p = 2 \\ \mathrm{diag}(1, -v, p), & p \text{ odd} \end{cases}$$

where v is a non-square p-adic unit

Unique p-adic rotation group on $\mathbb{Q}_p^3$:

$$\begin{aligned} \mathrm{SO}(3)_p :=& \mathrm{SO}(Q_+) \\ =& \left\{ L \in \mathrm{M}(3, \mathbb{Q}_p) \text{ s.t. } L^\top Q_+ L = Q_+,\ \det L = 1 \right\} \end{aligned}$$

No compact orthogonal groups on $\mathbb{Q}_p^n$ for $n \geq 5$

[2] Di Martino, Mancini, Pigliapochi, Svampa, Winter, "Geometry of the p-Adic Special Orthogonal Group $\mathrm{SO}(3)_p$", *Lobachevskii J. Math.* **44**(6), pp. 2135-2159 (2023).

Basic facts about $\mathrm{SO}(3)_p$

- $\mathrm{SO}(3)_p \subset \mathrm{M}(3, \mathbb{Z}_p)$ is compact

The elements of $\mathrm{SO}(3)_p$ are rotations $\mathcal{R}_{\boldsymbol{n}}$ around a fixed axis $\mathbb{Q}_p\boldsymbol{n}$ of $\mathbb{Q}_p^3$

- Given $\boldsymbol{n} \in \mathbb{Q}_p^3 \setminus \{0\}$, for any $\boldsymbol{v}$, $\boldsymbol{w} \in \boldsymbol{n}^\perp \setminus \{0\}$, there exists $\mathcal{R}_{\boldsymbol{n}} \in \mathrm{SO}(3)_p$ such that $\mathcal{R}_{\boldsymbol{n}}\boldsymbol{v} = \boldsymbol{w}$ if and only if $Q_+(\boldsymbol{v}) = Q_+(\boldsymbol{w})$.

For $p = 3$ (resp. $p > 3$), there are three (resp. two) groups

$$\mathrm{SO}(2)_{p,d} \simeq C_{-d} \leq \mathbb{Q}_p(\sqrt{-d})$$

$$\mathrm{SO}(2)_{3,1} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}_3, \qquad (\text{resp. } \mathrm{SO}(2)_{p,-v} \simeq \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}_p$$

$$\mathrm{SO}(2)_{3,-3} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_3, \qquad \mathrm{SO}(2)_{p,p} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_p\ )$$

$$\mathrm{SO}(2)_{3,3} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}_3,$$

Euler and nautical angles

Any $R \in \mathrm{SO}(3)_{\mathbb{R}}$ can be written as any of the compositions

$$R_x R_y R_z, \quad R_y R_z R_x, \quad R_z R_x R_y, \quad R_x R_z R_y, \quad R_z R_y R_x, \quad R_y R_x R_z$$
$$R_x R_y R_x, \quad R_x R_z R_x, \quad R_y R_x R_y, \quad R_y R_z R_y, \quad R_z R_x R_z, \quad R_z R_y R_z,$$

respectively of certain angles $\theta, \psi, \phi \in \mathbb{R}$

Theorem

Any $\mathcal{R} \in \mathrm{SO}(3)_p$, can be written as any of the compositions

$$\mathcal{R}_z\mathcal{R}_y\mathcal{R}_x, \quad \mathcal{R}_z\mathcal{R}_x\mathcal{R}_y, \quad \mathcal{R}_x\mathcal{R}_y\mathcal{R}_z, \quad \mathcal{R}_y\mathcal{R}_x\mathcal{R}_z,$$

respectively of certain parameters $\sigma, \tau, \omega \in \mathbb{Q}_p \cup \{\infty\}$

None of the other decompositions exist.

Each is exactly twofold, and unique if we restrict the parameters:

$$\mathcal{R} = \mathcal{R}_z(\omega)\mathcal{R}_y(\tau)\mathcal{R}_x(\sigma) = \mathcal{R}_z(\infty)\mathcal{R}_z(\omega)\mathcal{R}_y(\infty)\mathcal{R}_y(-\tau)\mathcal{R}_x(\infty)\mathcal{R}_x(\sigma)$$

Proof

$\mathcal{R} = \mathcal{R}_{\boldsymbol{n}_1}(\sigma)\mathcal{R}_{\boldsymbol{n}_2}(\tau)\mathcal{R}_{\boldsymbol{n}_3}(\omega)$ iff $\mathcal{R}_{\boldsymbol{n}_2}(\tau)^{-1}\mathcal{R}_{\boldsymbol{n}_1}(\sigma)^{-1}\mathcal{R}\boldsymbol{n}_3 = \boldsymbol{n}_3$
iff there exists $\mathcal{R}_{\boldsymbol{n}_1}(\sigma) \in \mathrm{SO}(3)_p$ s.t.

$$\mathcal{R}_{\boldsymbol{n}_1}(\sigma)^{-1}\mathcal{R}\boldsymbol{n}_3 \perp \boldsymbol{n}_2 \tag{1}$$

$$Q_+\left(\mathcal{R}_{\boldsymbol{n}_1}(\sigma)^{-1}\mathcal{R}\boldsymbol{n}_3\right) = Q_+(\boldsymbol{n}_3) \tag{2}$$

- E.g. $(\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{n}_3) = (\boldsymbol{e}_3, \boldsymbol{e}_2, \boldsymbol{e}_1)$
  Is there $x_1 \in \mathbb{Q}_p$ such that $x_1^2 + px_2^2 = 1$ where $x_2 \in \mathbb{Z}_p$?
  By Hensel's Lemma
- Non-existence with counterexamples on Eqs. (1), (2)
- Duplicity due to $\mathcal{R}_x(\infty)\mathcal{R}_y(\infty)\mathcal{R}_z(\infty) = \mathrm{I}_3$ and solutions of one quadratic equation in one unknown

p-Adic quaternions [3]

- The p-adic quaternion algebra $\mathbb{H}_p$ is the division algebra over $\mathbb{Q}_p$ with basis $(1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k} := \boldsymbol{ij})$ satisfying $\boldsymbol{i}^2 = v,\ \boldsymbol{j}^2 = -p,\ \boldsymbol{ji} = -\boldsymbol{ij}$
- $\mathbb{H}_p \ni \xi = q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$
- $\mathrm{nrd}(\xi) = Q_+^{(4)}((q_0, q_1, q_2, q_3))$

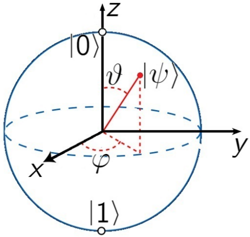
$$\mathrm{SO}(3)_p \simeq \mathbb{H}_p^\times / \mathbb{Q}_p^\times$$

[3] Aniello, L'Innocente, Mancini, Parisi, Svampa, Winter, "Invariant measures on p-adic Lie groups: the p-adic quaternion algebra and the Haar integral on the p-adic rotation groups", *Lett. Math. Phys.* **114**(78) (2024).

Euclidean scenario

$$\mathrm{SO}(3)_{\mathbb{R}} \simeq \mathrm{SU}(2)/\{\pm \mathrm{I}\}$$

- $(2l+1)$-dim irreps indexed by integer or half-integer l
- The state space of the qubit is $\mathbb{C}^2$
  Vector states on the Bloch sphere



- p-Adic qubit as a projective irrep of $\mathrm{SO}(3)_p$ on $\mathbb{C}^2$

$\mathrm{SO}(3)_p$ mod p^k [4]

- $\mathrm{SO}(3)_p \subset \mathrm{M}(3, \mathbb{Z}_p)$ is a profinite group
- Homomorphism for $k \in \mathbb{N}$:

$$\pi_k \colon \mathrm{SO}(3)_p \to \pi_k\big(\mathrm{SO}(3)_p\big) \subset \mathrm{M}(3,\, \mathbb{Z}/p^k\mathbb{Z})$$

$$\pi_k(\mathcal{R}) = \mathcal{R} \bmod p^k \qquad \text{entry-wise}$$

- Finite groups $G_{p^k} := \pi_k\big(\mathrm{SO}(3)_p\big)$

$$\dots \longrightarrow\!\!\!\!\rightarrow G_{p^{k+1}} \xrightarrow{\text{mod } p^k} G_{p^k} \longrightarrow\!\!\!\!\rightarrow \dots \longrightarrow\!\!\!\!\rightarrow G_{p^2} \xrightarrow{\text{mod } p} G_p$$

Inverse limit:

$$\mathrm{SO}(3)_p = \varprojlim \{G_{p^k}\}_{\mathbb{N}}$$

- $|G_{p^k}| = 2p^{3k-1}(p+1)$

[4] Aniello, L'Innocente, Mancini, Parisi, Svampa, Winter, "Characterising the Haar measure on the p-adic rotation groups via inverse limits of measure spaces", *Expo. Math.* **43**(2) (2025).

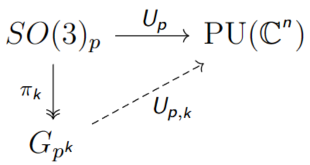
Factorisation of irreps

Irrep $U_{p,k}$ of G_{p^k} $\rightsquigarrow$ irrep U_p of $\mathrm{SO}(3)_p$

Proposition

For every irrep U_p of $\mathrm{SO}(3)_p$, there exists $k \in \mathbb{N}$, irrep $U_{p,k}$ of G_{p^k}, such that

$$U_p = U_{p,k} \circ \pi_k.$$



Proof:

- $\rho : G \to \mathrm{U}(n)$ continuous iff $\ker(\rho)$ open
- factorisation of ρ through $\ker(\pi_k) \subseteq \ker(\rho)$
- extend to projective representations $\underline{U} : G \to \mathrm{PU}(\mathbb{C}^n) = \mathrm{U}(n)/\mathrm{U}(1)$
  $\rho : G \to \mathrm{U}\big(\mathrm{M}(n, \mathbb{C})\big)$, $\rho(g)M := U(g)MU(g)^\dagger$

Irreps of G_p [5]

$$G_p = \left\{ \begin{pmatrix} a & svb & 0 \\ b & sa & 0 \\ c & d & s \end{pmatrix} \text{ s.t. } a^2 - vb^2 \equiv 1,\ s \equiv \pm 1 \bmod p \right\}$$

Semidirect product:

$$G_p \simeq N_{p^2} \rtimes H_{2(p+1)}$$

$$N_{p^2} := \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ c & d & 1 \end{pmatrix} \right\} \simeq \mathbb{Z}/p^2\mathbb{Z}, \quad H_{2(p+1)} := \left\{ \begin{pmatrix} a & svb & 0 \\ b & sa & 0 \\ 0 & 0 & s \end{pmatrix} \right\} \simeq \mathrm{D}_{p+1}$$

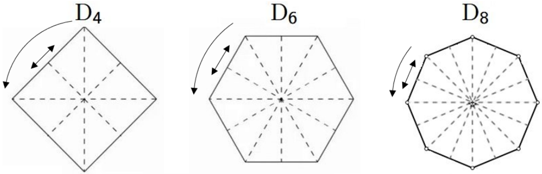
Method of little groups (Wigner, Mackey):

- Irreps from D_{p+1}
- other $2(p-1)$ $(p+1)$-dimensional irreps

[5] Svampa, Mancini, Winter, "An approach to p-adic qubits from irreducible representations of $\mathrm{SO}(3)_p$", *J. Math. Phys.* **63**(7), 2022.

p-Adic qubit representations

Onto homomorphism $\phi_p \colon G_p \to \mathrm{D}_{p+1}$



$\dots$

D_{p+1} has:

four 1-dim irreps

$\frac{p-1}{2}$ 2-dim irreps $\sigma_p^{(i)}$

$\Downarrow$

many p-adic qubits for $p > 3$

p-Adic qubits:

$$U_p^{(i)} \colon \mathrm{SO}(3)_p \to \mathrm{U}(2), \qquad U_p^{(i)} := \sigma_p^{(i)} \circ \phi_p \circ \pi_1$$

p-Adic quantum computing [6]

- The p-adic qubit is the fundamental object
- Its pure states are on $\mathbb{C}^2$
- Composite systems of qubits via tensor-product representations
- Clebsch-Gordan decomposition

Standard QM

Unique 2-dim irrep U

$U^{\otimes n} \rightsquigarrow$ all irreps

p-Adic QM

More 2-dim irreps

$U_p = U_{p,k} \circ \pi_k \Rightarrow U_p^{\otimes n} = U_{p,k}^{\otimes n} \circ \pi_k$

[6] Svampa, L'Innocente, Mancini, Winter, "Composing p-adic qubits: from representations of $\mathrm{SO}(3)_p$ to entanglement and universal quantum logic gates", arXiv:2601.13808.

p-Adic quantum information [6]

- Clebsch-Gordan decomposition

Standard QM

$2 \otimes 2 \simeq 1 \oplus 3$

p-Adic QM

For the 2-dim irreps of D_{p+1}:

$2 \otimes 2 \simeq 1 \oplus 1 \oplus 1 \oplus 1$

$2 \otimes 2 \simeq 1 \oplus 1 \oplus 2$

$2 \otimes 2 \simeq 2 \oplus 2$

- Entanglement

Singlet $|\Psi^-\rangle$

Triplet $(|00\rangle, |\Psi^+\rangle, |11\rangle)$

Singlets or doublets

$|\Phi^\pm\rangle, |\Psi^\pm\rangle$

where $|\Phi^\pm\rangle := \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\Psi^\pm\rangle := \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are the four maximally entangled Bell states

[6] L'Innocente, Mancini, Svampa, Winter, "Putting together p-adic qubits: from representations of $\mathrm{SO}(3)_p$ to entanglement and logic gates", in preparation.

p-Adically controlled logic gates

- Circuit model of quantum computation
- Gates on n qubits by irreps of $\mathrm{SO}(3)_p$ on $\mathrm{U}(2^n)$
- GAP for character table and irreps of G_3
- Entangling 2-qubit gates

Universal set:

$$\mathcal{G}_1\mathfrak{p}_3 := \left\{ X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, S := \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, \widetilde{CZ} := \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\}$$

Conclusions

- There is a unique group $\mathrm{SO}(3)_p$.
  We studied its geometric and topological properties: rotations, nautical decompositions, inverse limit, quaternions, Hensel's lift.
- We studied the irreps of $\mathrm{SO}(3)_p$.
  They all factorise modulo p^k for some k.
  We found explicit p-adic qubit representations for every prime p.
- We laid the foundations of a p-adic theory of angular momentum and spin, as well as of p-adically controlled quantum computation

Open questions

- KAK or Cartan decomposition of $\mathrm{SO}(3)_p$
- Classify all the irreps of $\mathrm{SO}(3)_p$
  Kirillov (and Howe) orbit method
  Haar measure
- Number of 1-dim irreps
  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subseteq \mathrm{SO}(3)_p/[\mathrm{SO}(3)_p, \mathrm{SO}(3)_p]$
  Number of 2-dim irreps $\leftrightarrow$ p-adic qubits
- Composite system of more than two p-adic qubit

$p = 2$

- Unique $Q_+ \doteq \mathrm{I}_3$ and $\mathrm{SO}(3)_2$,
- three groups $\mathrm{SO}(2)_{2,d}$

$$\mathrm{SO}(2)_{2,-5} \subset \mathrm{SL}(2, 2^{-1}\mathbb{Z}_2)$$

- No Euler or nautical decomposition for $\mathrm{SO}(3)_2$
- Multivariable Hensel's lift does not work
- Unique 2-adic qubit from $G_2 \simeq \mathrm{D}_3$
  $2 \otimes 2 \simeq 1 \oplus 1 \oplus 2$
  No 4-dim irrep

Thank You!