P-adic Coding and Computations

Thomas Liebig

Smart City Science

- „real-time systems for public good connecting public sector with industrial sector“

Aspects

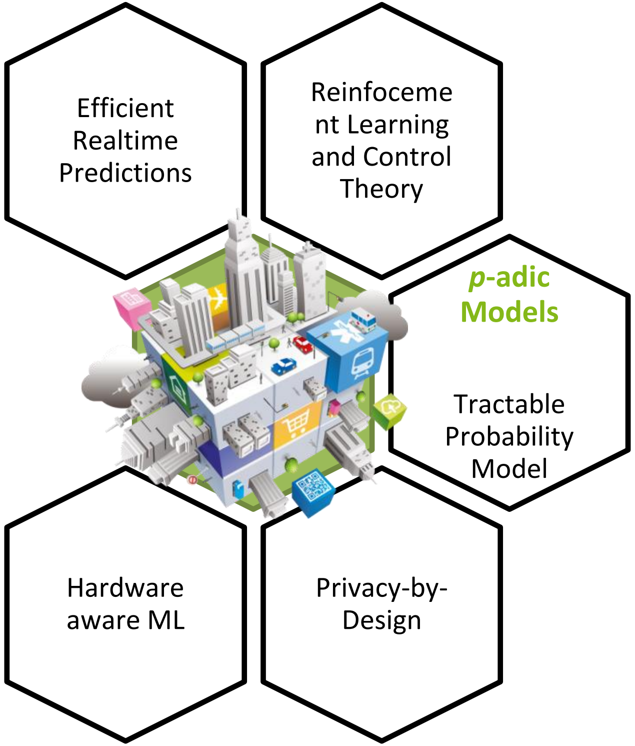
- Standards
- Systems
  Realtime, Distributed
- Governance balkanization
  Gaia-X, architecture, Geo-spatial IOT, …
- Algorithms/Methods
  Distributed, Tractable, Efficient, Adequate, Ressource Aware
- Ethics
  Privacy, Explainability, Participation and Knowledge Transfer

Smart City Science Topics

N.N.

Xeniya Gusseva (BSc)
  HiWi (SFB-B4)

Fried Kullman (MSc)
  Prediction of Machine State after Fault Injection



N.N.

Karen Toben (MSc)
  p-adic Neural Networks

Lukas Schneider (BSc)
  Factorizing Distributions by Conditional Sum Product Networks

Timon Sachweh (MSc)
  Differential Privacy for Learning from Label Proportions

Prediction of traffic flow

Models and their Assumptions:

- Spatio-Temporal Random Fields
  - Markov Assumption
  - Tobler‘s Law
  - Daily Routines
- Distributed Prediction
  - Tobler‘s Law
- Gaussian Process Regression
  - Central limit theorem
  - Tobler‘s Law
- Graph CNN
  - Markov Assumption
  - Tobler‘s Law
  - Network topology
- Conditional Sum-Product Networks
  - Discrete distribution
  - Markov Assumption

We made implicit Assumptions

- Since Newton/Leibniz Spatio-Temporal phenomena modelled by ODE or PDE on $\mathbb{R}$ (Euclidean or Minkowski coordinates)
- Models in $\mathbb{R}$ map to $\mathbb{R}$
- Veronese & Hilbert stated in Euclidean geometry holds Archimedean Axiom

$$b > a \Rightarrow \exists m : b < m \cdot a$$

Problem with these Assumptions

- But, our observations can not be infinitesimal and are bound to topology of traffic network

→ Abandon Archimedean Axiom at very small scale (e.g. innercity junctions with low temporal granularity)

- How?

Geometry and Number Systems

- Coordinates describe Geometric picture

  $\mathbb{R}$ Euclidean geometry

  ? Non-Euclidean geometry

- In computations or for measurements we use $\mathbb{Q}$

→ field $(\mathbb{Q}, |\cdot|)$

$$|x| = 0 \iff x = 0$$
$$|xy| = |x||y|$$
$$|x + y| \leq |x| + |y|$$

Two Possibilities for |·| [Ostrowski 16]

$$|\cdot| : \mathbb{Q} \mapsto \mathbb{Q}_+$$

$$|x| = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases}$$

- Completion of $(\mathbb{Q}, |\cdot|)$ leads to

$(\mathbb{R}, |\cdot|)$

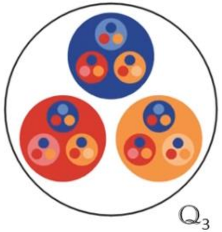
The Geometry of $\mathbb{Q}_p$

- $\mathbb{R}$ and $\mathbb{Q}_p$ are metric spaces
- $(\mathbb{R}, |\cdot|)$ and $(\mathbb{Q}_p, |\cdot|_p)$ are very different!
- In a metric space $(\mathbb{X}, d)$ the open balls are sets

$$U_r = \{x \in \mathbb{X} : d(a, x) < r\}$$

in $(\mathbb{R}, |\cdot|)$ $$U_r = \{x \in \mathbb{R} : |a - x| < r\} = (a - r, a + r)$$

in $(\mathbb{Q}_p, |\cdot|_p)$ $$U_r = \{x \in \mathbb{Q}_p : |a - x|_p < r\}$$



Applications of *p*-adic Models

- Turbulence
- Dynamic Systems
- Cryptography
- Economy
- Chaotic Fractal Behavior
- Quantum Mechanics
- Hierachical Models
- Neuro Cognition

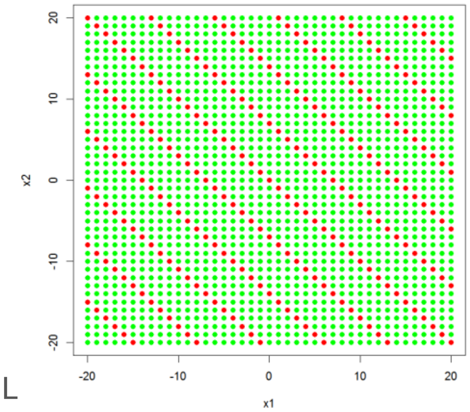
Classification of p-adic vectors

$$\mathbb{Q}_p^N = \mathbb{Q} \times \mathbb{Q} \times \ldots \times \mathbb{Q}$$

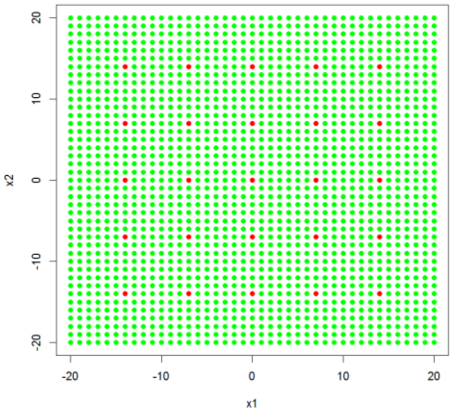
$$\|x\|_p = max|x_j|_p \text{ with: } x = (x_0, \ldots, x_{N-1}) \in \mathbb{Q}_p^N$$

- Example $x = (x_1, x_2)^T \in \mathbb{Q}_7^2$

$|x_1 + x_2|_7 < 0.5$



$\|x\|_7 < 0.5$

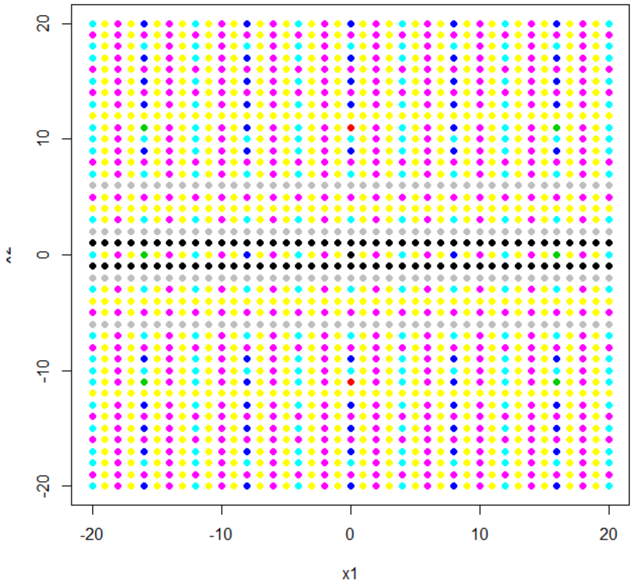


Classification of p-adic vectors

- Sphere

$$||x \cdot c^T||_2 - b = 0$$

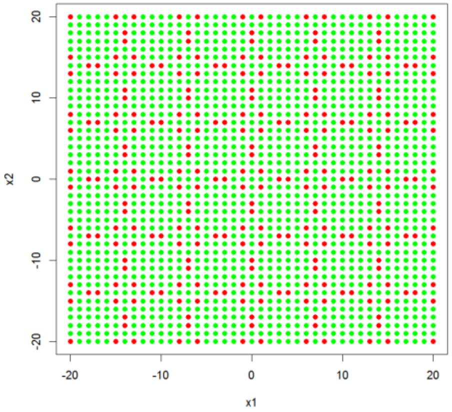
selects one of these colors



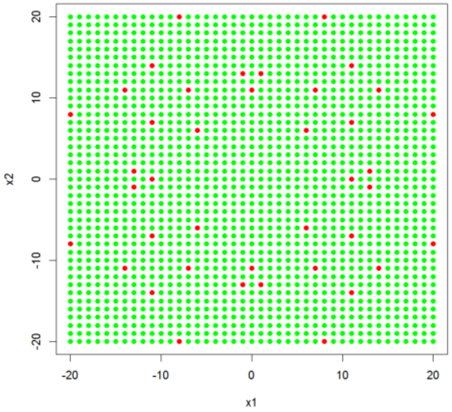
Classification by digits of p-adic extension

$$x = (x_1, x_2)^T \in \mathbb{Q}_7^2$$

$$[x_1^2 + x_2^2]_7 \stackrel{?}{=} 2\ldots$$



$$[x_1^2 + x_2^2]_7 \stackrel{?}{=} 23\ldots$$



Negative probabilities

- In Kolmogorovs probability framework probabilities of events must be **positive real numbers** [Kolmogorov 31]
- Here, we consider ensemble frequency of an ensemble of balls [Mises 19]
  - Consider, countable number of colors C
  - We observe an ensemble S of colored balls with the #num of balls per color $k = 2^k$

Negative probabilities

- Here, we consider ensemble frequency of an ensemble of balls
  - Consider, countable number of colors
  - We observe an ensemble *S* of colored balls with the #num of balls per color *k* $=2^k$

- ‚Volume' $N = |S|$ of S is

$$N = \sum_{k=0}^{\infty} n_k = \sum_{k=0}^{\infty} 2^k$$

Negative probabilities

- This sum diverges in $\mathbb{R}$

$$N = \sum_{k=0}^{\infty} n_k = \sum_{k=0}^{\infty} 2^k$$

but converges in $\mathbb{Q}_2$

$$N = \sum_{k=0}^{\infty} 2^k = \frac{1}{1-2} = -1$$

Interesting to explore

- Models in $\mathbb{Q}_p$
- Model for (chaotic) cellular automaton (e.g. sandpile avalanche process)
- Negative & complex probabilities
  Description of Quasiprobabilities (e.g. Wigner distribution)
- Utilization of p-adic Algorithms in ressource constraint devices e.g. matrix inversion by [Dixon 82] ring inversion [Koç 17] random graphs [Hua & Hovestadt 21]

Literature

- Dixon, J. D. (1982). Exact solution of linear equations using p-adic expansions. *Numerische Mathematik*, *40*(1), 137-141.
- Hilbert, D. (1899). Grundlagen der Geometrie: 14c. *Auflage. BG Teubner.(Original work published in 1899).[KKN]*.
- Hensel, K. (1897). Über eine neue Begründung der Theorie der algebraischen Zahlen. Jahresbericht der Deutschen Mathematiker-Vereinigung, 6, 83-88.
- Hua, H., & Hovestadt, L. (2021). p-adic numbers encode complex networks. *Scientific Reports*, *11*(1), 1-11.
- Khrennikov, A. (2009). *Interpretations of probability*. Walter de Gruyter.
- Koç, C. K. (2017). A New Algorithm for Inversion mod p^k. *IACR Cryptol. ePrint Arch.*, *2017*, 411.
- Kolmogoroff, A. (1931). Über die analytischen Methoden in der Wahrscheinlichkeitsrechnung. *Mathematische Annalen*, *104*(1), 415-458.
- Mises, R. V. (1919). Grundlagen der Wahrscheinlichkeitsrechnung. *Mathematische Zeitschrift*, *5*(1), 52-99.
- Ostrowski, A. (1916). Über einige Lösungen der Funktionalgleichung ψ (x)· ψ (x)= ψ (xy). *Acta Mathematica*, *41*(1), 271-284.
- Veronese, G., & Schepp, A. (1894). *Grundzüge der Geometrie von mehreren Dimensionen und mehreren Arten gradliniger Einheiten in elementarer Form entwickelt*. BG Teubner.