Estimating a p-adic volume via coin problems

Joe Webster

University of Oregon

February 10, 2020

Motivating question

- Fix a prime number p and an integer $N \geq 2$.
- For each tuple $\boldsymbol{x} = (x_1, x_2, \ldots, x_N) \in \mathbb{Z}_p^N$, define

$$\Delta(\boldsymbol{x}) := \prod_{1 \leq i < j \leq N} |x_i - x_j|_p$$

- Note $\Delta(\boldsymbol{x}) \in \{1, \frac{1}{p}, \frac{1}{p^2}, \frac{1}{p^3}, \ldots\} \cup \{0\}$ for all $\boldsymbol{x} \in \mathbb{Z}_p^N$.
- **Question:** Given $n \in \mathbb{Z}_{\geq 0}$, if $\boldsymbol{x}$ is chosen from $\mathbb{Z}_p^N$ uniformly randomly, what is the probability that $\Delta(\boldsymbol{x}) = p^{-n}$?

What does "coin problem" mean?

Fix a finite set of pairwise coprime "coin sizes" $c_1, c_2, \ldots, c_\ell \in \mathbb{N}$ and let $\boldsymbol{c} = (c_1, c_2, \ldots, c_\ell)$. For each integer $m \geq 0$, define

$$\mathcal{P}_{\boldsymbol{c},m} := \{(k_1, k_2, \ldots, k_\ell) \in \mathbb{Z}_{\geq 0}^\ell : c_1 k_1 + c_2 k_2 + \cdots + c_\ell k_\ell = m\} .$$

Examples of coin problems include:

- What is the largest m such that $\mathcal{P}_{\boldsymbol{c},m} = \varnothing$?
- What is $\#\mathcal{P}_{\boldsymbol{c},m}$ as a function of m?
- How can we describe/parametrize generic elements of $\mathcal{P}_{\boldsymbol{c},m}$?

All of these problems are hard unless $\ell \in \{1, 2\}$.

The precise question and today's goals

If μ is the Haar measure on $\mathbb{Z}_p$ satisfying $\mu(\mathbb{Z}_p) = 1$, the probability we want is given by

$$\mathbb{P}\{\Delta(\boldsymbol{x}) = p^{-n}\} = \mu^N(\Delta^{-1}(p^{-n})) \ .$$

How does it vary with N, p, and n?

- **Goal 1**: Derive an effective formula for $\mu^N(\Delta^{-1}(p^{-n}))$.
- **Goal 2**: Use the formula in the $N = 2$ and $N = 3$ cases.
- **Goal 3**: Get an explicit bound for general N, p, and n.

Series representations for $\boldsymbol{x} \in \mathbb{Z}_p^N$

- For each $\boldsymbol{x} \in \mathbb{Z}_p^N$, there is a unique sequence of tuples $(\boldsymbol{d}(m))_{m \geq 0}$ satisfying $d_i(m) \in \{0, 1, \ldots, p-1\}$ and

  $$x_i = d_i(0) + d_i(1)p + d_i(2)p^2 + d_i(3)p^3 + \ldots$$

  for all $i \in \{1, 2, \ldots, N\}$.

- Key fact: If $x_i \neq x_j$, then

  $$|x_i - x_j|_p = p^{-k} \quad \Longleftrightarrow \quad \min\{m : d_i(m) \neq d_j(m)\} = k.$$

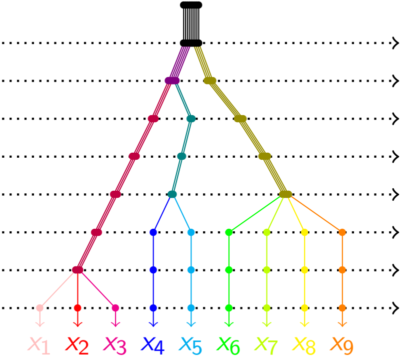
- In particular, if $\Delta(\boldsymbol{x}) \neq 0$, then

  $$\Delta(\boldsymbol{x}) = p^{-n} \quad \Longleftrightarrow \quad \sum_{1 \leq i < j \leq N} \min\{m : d_i(m) \neq d_j(m)\} = n.$$

Example: A tuple $\boldsymbol{x} \in \mathbb{Z}_5^9$ with $\Delta(\boldsymbol{x}) \neq 0$.

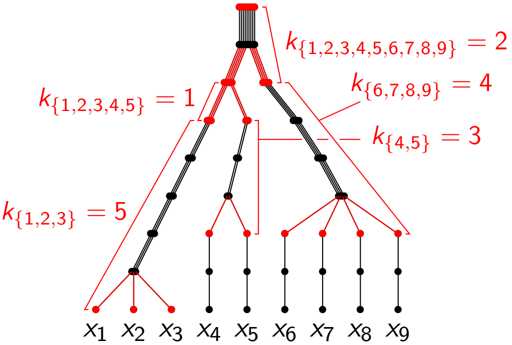
Suppose $\boldsymbol{x} = \boldsymbol{d}(0) + 5\boldsymbol{d}(1) + 5^2\boldsymbol{d}(2) + 5^3\boldsymbol{d}(3) + \dots$, where

$$\boldsymbol{d}(0) = (2, 2, 2, 2, 2, 2, 2, 2, 2)$$
$$\boldsymbol{d}(1) = (0, 0, 0, 0, 0, 3, 3, 3, 3)$$
$$\boldsymbol{d}(2) = (3, 3, 3, 4, 4, 1, 1, 1, 1)$$
$$\boldsymbol{d}(3) = (2, 2, 2, 1, 1, 0, 0, 0, 0)$$
$$\boldsymbol{d}(4) = (4, 4, 4, 0, 0, 4, 4, 4, 4)$$
$$\boldsymbol{d}(5) = (1, 1, 1, 2, 4, 0, 1, 3, 4)$$
$$\boldsymbol{d}(6) = (0, 0, 0, 4, 3, 3, 2, 2, 0)$$
$$\boldsymbol{d}(7) = (0, 1, 4, 3, 4, 2, 1, 1, 1)$$
$$\vdots$$



Example (continued): The "shape" of $\boldsymbol{x}$

The tree defines a set of "branches" $\mathcal{B}$...
...and a corresponding tuple $\boldsymbol{k} \in \mathbb{N}^{\mathcal{B}}$.



$$\mathcal{B} = \left\{ \begin{array}{r} \{1,2,3,4,5,6,7,8,9\} \\ \{1,2,3,4,5,6,7,8,9\} \\ \{1,2,3,4,5\}\{6,7,8,9\} \\ \{1,2,3\}\{4,5\}\{6,7,8,9\} \\ \{1,2,3\}\{4,5\}\{6,7,8,9\} \\ \{1,2,3\}\{4,5\}\{6,7,8,9\} \\ \{1,2,3\}\{4\}\{5\}\{6\}\{7\}\{8\}\{9\} \\ \{1,2,3\}\{4\}\{5\}\{6\}\{7\}\{8\}\{9\} \\ \{1\}\{2\}\{3\}\{4\}\{5\}\{6\}\{7\}\{8\}\{9\} \end{array} \right\}$$

Call $(\mathcal{B}, \boldsymbol{k})$ the *shape* of $\boldsymbol{x}$.

Example (continued): $\Delta(x)$ depends on $(\mathcal{B}, \boldsymbol{k})$ alone

- **Key fact:** Our series for $\boldsymbol{x} \in \mathbb{Z}_5^9$ satisfies

$$\sum_{1\le i<j\le 9} \min\{m : d_i(m) \neq d_j(m)\} = -\binom{9}{2} + \sum_{\lambda\in\mathcal{B}} \binom{\#\lambda}{2} k_\lambda$$
$$= \binom{9}{2}\cdot(2-1) + \binom{5}{2}\cdot 1 + \binom{4}{2}\cdot 4 + \binom{2}{2}\cdot 3 + \binom{3}{2}\cdot 5 = 88,$$

- Therefore $\Delta(\boldsymbol{x}) = 5^{-88}$.

Branches and branch sets

Definition

Given $N \geq 2$, a *branch set* $\mathcal{B}$ of order N is a collection of subsets $\lambda \subset [N] = \{1, 2, \ldots, N\}$ (called *branches*) satisfying

(i) $[N] \in \mathcal{B}$,

(ii) $\#\lambda \geq 2$ for all $\lambda \in \mathcal{B}$, and

(iii) if $\lambda_1, \lambda_2 \in \mathcal{B}$ satisfy $\lambda_1 \cap \lambda_2 \neq \varnothing$, then $\lambda_1 \subset \lambda_2$ or $\lambda_1 \supset \lambda_2$.

Write $\mathcal{R}_N$ for the set of all branch sets of order N.

- **Ex:** $\mathcal{B} = \big\{[9], \{1,2,3,4,5\}, \{6,7,8,9\}, \{4,5\}, \{1,2,3\}\big\} \in \mathcal{R}_9$

- **Fact:** $1 \leq \#\mathcal{R}_N \leq 2^{N-1}(N-1)!$ for all $N \geq 2$.

Some technical definitions

Definition

The *degree* of a branch $\lambda \in \mathcal{B}$ is defined by

$$\deg_{\mathcal{B}}(\lambda) = \#\lambda - \sum_{\lambda'} (\#\lambda' - 1),$$

where the sum $\sum_{\lambda'}$ is over all maximal $\lambda' \in \mathcal{B}$ such that $\lambda' \subsetneq \lambda$.

Definition

Given a prime p, the *p-multiplicity* $M_{\mathcal{B},p}$ of a branch set $\mathcal{B}$ is

$$M_{\mathcal{B},p} := \prod_{\lambda \in \mathcal{B}} (p-1)_{\deg_{\mathcal{B}}(\lambda)-1} \ .$$

- **Fact:** If $\mathcal{B} \in \mathcal{R}_N$, then $0 \leq M_{\mathcal{B},p} \leq ((p-1)!)^{N-1}$ for all p.

Theorem (W.)

For each $\mathcal{B} \in \mathcal{R}_N$ and every $\boldsymbol{k} \in \mathbb{N}^{\mathcal{B}}$, define

$$\mathcal{T}(\mathcal{B}, \boldsymbol{k}) := \{\boldsymbol{x} \in \mathbb{Z}_p^N : \boldsymbol{x} \text{ has shape } (\mathcal{B}, \boldsymbol{k})\} \ .$$

(a) We have a countable decomposition

$$\mathbb{Z}_p^N = \Delta^{-1}(0) \sqcup \bigsqcup_{\mathcal{B} \in \mathcal{R}_N} \bigsqcup_{\boldsymbol{k} \in \mathbb{N}^{\mathcal{B}}} \mathcal{T}(\mathcal{B}, \boldsymbol{k}) \ .$$

(b) Each $\mathcal{T}(\mathcal{B}, \boldsymbol{k})$ is open and compact with measure

$$\mu^N(\mathcal{T}(\mathcal{B}, \boldsymbol{k})) = M_{\mathcal{B},p} \cdot \prod_{\lambda \in \mathcal{B}} p^{-(\#\lambda - 1)k_\lambda} \ .$$

(c) We have $\Delta(\boldsymbol{x}) = p^{\binom{N}{2} - \sum_{\lambda \in \mathcal{B}} \binom{\#\lambda}{2} k_\lambda}$ for all $\boldsymbol{x} \in \mathcal{T}(\mathcal{B}, \boldsymbol{k})$.

An exact solution in terms of shapes

Corollary

For any $N \geq 2$, prime p, and integer m, we have

$$\mu^N(\Delta^{-1}(p^{\binom{N}{2}-m})) = \sum_{\mathcal{B}\in\mathcal{R}_N} M_{\mathcal{B},p} \cdot \sum_{\boldsymbol{k}\in\mathcal{K}_{\mathcal{B},m}} \prod_{\lambda\in\mathcal{B}} p^{-(\#\lambda-1)k_\lambda}$$

where

$$\mathcal{K}_{\mathcal{B},m} := \left\{ \boldsymbol{k} \in \mathbb{N}^{\mathcal{B}} : \sum_{\lambda\in\mathcal{B}} \binom{\#\lambda}{2} k_\lambda = m \right\}.$$

- **Fact:** If $\mathcal{B} \in \mathcal{R}_N$ and $m \geq \binom{N}{2}$, then $\#\mathcal{K}_{\mathcal{B},m} \leq m^{\#\mathcal{B}} \leq m^{N-1}$.

Example: $N = 2$

(i) $\mathcal{B} = \big\{\{1,2\}\big\}$ is the only branch set of order 2.

(ii) The p-multiplicity is $M_{\mathcal{B},p} = (p-1)_{2-1} = p - 1 > 0$ for all p.

(iii) $\mathcal{K}_{\mathcal{B},m} = \{k \in \mathbb{N} : k = m\} = \begin{cases} \{m\} & \text{if } m \geq 1, \\ \varnothing & \text{otherwise.} \end{cases}$

Then $\mu^2(\Delta^{-1}(p^{1-m})) = (p-1) \cdot p^{-(2-1)m} = \frac{p-1}{p^m}$ if $m \geq 1$, so

$$\mathbb{P}\{\Delta(\boldsymbol{x}) = p^{-n}\} = \frac{p-1}{p^{n+1}} \ .$$

Example: $N = 3$

(i) All branch sets of order 3:

$$\begin{aligned} \mathcal{B}_0 &= \big\{\{1,2,3\}\big\}, \\ \mathcal{B}_1 &= \big\{\{1,2,3\},\{1,2\}\big\}, \\ \mathcal{B}_2 &= \big\{\{1,2,3\},\{1,3\}\big\}, \\ \mathcal{B}_3 &= \big\{\{1,2,3\},\{2,3\}\big\}. \end{aligned}$$

(ii) The corresponding p-multiplicities:

$$\begin{aligned} M_{\mathcal{B}_0,p} &= (p-1)_2 \qquad (= 0 \text{ if } p = 2), \\ M_{\mathcal{B}_1,p} &= (p-1)^2, \\ M_{\mathcal{B}_2,p} &= (p-1)^2, \\ M_{\mathcal{B}_3,p} &= (p-1)^2. \end{aligned}$$

Example: $N = 3$ (continued)

(iii) Since

$$\mathcal{K}_{\mathcal{B}_0,m} = \{k \in \mathbb{N} : 3k = m\} = \begin{cases} \{m/3\} & \text{if } m \in 3\mathbb{N}, \\ \varnothing & \text{otherwise,} \end{cases}$$

we get a summand

$$M_{\mathcal{B}_0,p} \cdot \sum_{\boldsymbol{k} \in \mathcal{K}_{\mathcal{B}_0,m}} \prod_{\lambda \in \mathcal{B}_0} p^{-(\#\lambda - 1)k_\lambda} = \mathbf{1}_{3\mathbb{N}}(m)(p-1)_2 p^{-2m/3} .$$

For each $i \in \{1, 2, 3\}$ we have

$$\begin{aligned} \mathcal{K}_{\mathcal{B}_i,m} &= \left\{(k_1, k_2) \in \mathbb{N}^2 : 3k_1 + k_2 = m\right\} \\ &= \{(k, m-3k) : 1 \le k \le \lfloor (m-1)/3 \rfloor\} \end{aligned}$$

and we get a summand

$$M_{\mathcal{B}_i,p} \cdot \sum_{\boldsymbol{k} \in \mathcal{K}_{\mathcal{B}_i,m}} \prod_{\lambda \in \mathcal{B}_i} p^{-(\#\lambda - 1)k_\lambda} = (p-1)^2 p^{-m} \sum_{k=1}^{\lfloor (m-1)/3 \rfloor} p^k .$$

Example: $N = 3$ (continued)^2

Thus, for $m \geq 3$ we have

$$\mu^3(\Delta^{-1}(p^{3-m})) = \mathbf{1}_{3\mathbb{N}}(m)(p-1)_2 p^{-2m/3} + 3(p-1)^2 p^{-m} \sum_{k=1}^{\lfloor (m-1)/3 \rfloor} p^k$$

and hence

$$\mathbb{P}\{\Delta(\boldsymbol{x}) = p^{-n}\} = \mathbf{1}_{3\mathbb{N}}(n+3)(p-1)_2 p^{-2(n+3)/3} + 3(p-1)^2 p^{-(n+3)} \sum_{k=1}^{\lfloor (n+2)/3 \rfloor} p^k.$$

Challenges in the $N \geq 4$ cases

- When $N \geq 4$, there are $\mathcal{B} \in \mathcal{R}_N$ with $\#\mathcal{B} \geq 3$ and $M_{\mathcal{B},p} > 0$.
- In order to calculate the summand for such $\mathcal{B}$, we would need to explicitly describe all elements of

$$\mathcal{K}_{\mathcal{B},m} := \left\{ \boldsymbol{k} \in \mathbb{N}^{\mathcal{B}} : \sum_{\lambda \in \mathcal{B}} \binom{\#\lambda}{2} k_\lambda = m \right\}.$$

- Even if all $\binom{\#\lambda}{2}$ are relatively prime, this is an open problem!
- For large N, it is also challenging to tabulate all $\mathcal{B} \in \mathcal{R}_N$ and their corresponding p-multiplicities.

The good news for general N, p, and n:

Recall the (crude) bounds from before:

- $\#\mathcal{R}_N \leq 2^{N-1}(N-1)!$ for all $N \geq 2$
- $M_{\mathcal{B},p} \leq ((p-1)!)^{N-1}$ for all $N \geq 2$ and all p
- $\#\mathcal{K}_{\mathcal{B},m} \leq m^{N-1}$ for all $\mathcal{B} \in \mathcal{R}_N$ and all $m \geq \binom{N}{2}$
- If $\boldsymbol{k} \in \mathcal{K}_{\mathcal{B},m}$, then $\prod_{\lambda\in\mathcal{B}} p^{-(\#\lambda-1)k_\lambda} \leq p^{-\frac{2m}{N}}$.

Corollary

For any integers $N \geq 2$ and $m \geq \binom{N}{2}$ and any prime p, we have

$$\mu^N(\Delta^{-1}(p^{\binom{N}{2}-m})) \leq (2m(p-1)!)^{N-1}(N-1)!p^{-\frac{2m}{N}} \ .$$

A fun last remark

Given N and p, there is a positive constant $C(N,p)$ such that

$$\mathcal{P}\{\Delta(\boldsymbol{x}) = p^{-n}\} \leq C(N,p) \cdot p^{-\frac{n}{N}} \qquad \text{for all } n \geq 0.$$

Thank you!