Estimating a $p$-adic volume via coin problems

Joe Webster

University of Oregon

February 10, 2020
Fix a prime number $p$ and an integer $N \geq 2$.

For each tuple $x = (x_1, x_2, \ldots, x_N) \in \mathbb{Z}_p^N$, define

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

Note $\Delta(x) \in \{1, \frac{1}{p}, \frac{1}{p^2}, \frac{1}{p^3}, \ldots \} \cup \{0\}$ for all $x \in \mathbb{Z}_p^N$.

**Question:** Given $n \in \mathbb{Z}_{\geq 0}$, if $x$ is chosen from $\mathbb{Z}_p^N$ uniformly randomly, what is the probability that $\Delta(x) = p^{-n}$?
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 $c = (c_1, c_2, \ldots, c_\ell)$. For each integer $m \geq 0$, define

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

Examples of coin problems include:

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

All of these problems are hard unless $\ell \in \{1, 2\}$. 
If $\mu$ is the Haar measure on $\mathbb{Z}_p$ satisfying $\mu(\mathbb{Z}_p) = 1$, the probability we want is given by

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

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 $n$. 
For each \( x \in \mathbb{Z}_p^N \), there is a unique sequence of tuples \((d(m))_{m \geq 0}\) 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

\[
| x_i - x_j |_p = p^{-k} \iff \min \{ m : d_i(m) \neq d_j(m) \} = k.
\]

In particular, if \( \Delta(x) \neq 0 \), then

\[
\Delta(x) = p^{-n} \iff \sum_{1 \leq i < j \leq N} \min \{ m : d_i(m) \neq d_j(m) \} = n.
\]
Example: A tuple $x \in \mathbb{Z}_5^9$ with $\Delta(x) \neq 0$.

Suppose $x = d(0) + 5d(1) + 5^2d(2) + 5^3d(3) + \ldots$, where

- $d(0) = (2, 2, 2, 2, 2, 2, 2, 2, 2)$
- $d(1) = (0, 0, 0, 0, 0, 3, 3, 3, 3)$
- $d(2) = (3, 3, 3, 4, 4, 1, 1, 1, 1)$
- $d(3) = (2, 2, 2, 1, 1, 0, 0, 0, 0)$
- $d(4) = (4, 4, 4, 0, 0, 4, 4, 4, 4)$
- $d(5) = (1, 1, 1, 2, 4, 0, 1, 3, 4)$
- $d(6) = (0, 0, 0, 4, 3, 3, 2, 2, 0)$
- $d(7) = (0, 1, 4, 3, 4, 2, 1, 1, 1)$
- $\vdots$
The tree defines a set of “branches” $\mathcal{B}$... ...and a corresponding tuple $k \in \mathbb{N}^\mathcal{B}$.

\[ k_{\{1,2,3\}} = 5 \]
\[ k_{\{1,2,3,4,5\}} = 1 \]
\[ k_{\{4,5\}} = 3 \]
\[ k_{\{6,7,8,9\}} = 4 \]
\[ k_{\{1,2,3,4,5,6,7,8,9\}} = 2 \]

Call $(\mathcal{B}, k)$ the shape of $x$. 
Example (continued): $\Delta(x)$ depends on $(B, k)$ alone

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

$$\sum_{1 \leq i < j \leq 9} \min \{ m : d_i(m) \neq d_j(m) \} = -\binom{9}{2} + \sum_{\lambda \in B} \binom{\# \lambda}{2} k_{\lambda}$$

$$= \binom{9}{2} \cdot (2 - 1) + \binom{5}{2} \cdot 1 + \binom{4}{2} \cdot 4 + \binom{2}{2} \cdot 3 + \binom{3}{2} \cdot 5 = 88,$$

• Therefore $\Delta(x) = 5^{-88}$. 
Branches and branch sets

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

(i) $[N] \in B$,
(ii) $\#\lambda \geq 2$ for all $\lambda \in B$, and
(iii) if $\lambda_1, \lambda_2 \in B$ satisfy $\lambda_1 \cap \lambda_2 \neq \emptyset$, 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:** $B = \{[9], \{1, 2, 3, 4, 5\}, \{6, 7, 8, 9\}, \{4, 5\}, \{1, 2, 3\}\} \in \mathcal{R}_9$

- **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 $k \in \mathbb{N}^B$, define

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

(a) We have a countable decomposition

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

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

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

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

Corollary

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

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

where

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

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

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

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

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

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

$$
\mathbb{P}\{\Delta(x) = p^{-n}\} = \frac{p-1}{p^{n+1}}.
$$
Example: \( N = 3 \)

(i) All branch sets of order 3:

\[
B_0 = \{\{1, 2, 3\}\},
\]
\[
B_1 = \{\{1, 2, 3\}, \{1, 2\}\},
\]
\[
B_2 = \{\{1, 2, 3\}, \{1, 3\}\},
\]
\[
B_3 = \{\{1, 2, 3\}, \{2, 3\}\}.
\]

(ii) The corresponding \( p \)-multiplicities:

\[
M_{B_0,p} = (p - 1)^2 \quad (= 0 \text{ if } p = 2),
\]
\[
M_{B_1,p} = (p - 1)^2,
\]
\[
M_{B_2,p} = (p - 1)^2,
\]
\[
M_{B_3,p} = (p - 1)^2.
\]
(iii) Since

\[ \mathcal{K}_{B_0,m} = \{ k \in \mathbb{N} : 3k = m \} = \begin{cases} \{ m/3 \} & \text{if } m \in 3\mathbb{N}, \\ \emptyset & \text{otherwise,} \end{cases} \]

we get a summand

\[ M_{B_0,p} \cdot \sum_{k \in \mathcal{K}_{B_0,m}} \prod_{\lambda \in B_0} p^{-(\#\lambda-1)k_\lambda} = 1_{3\mathbb{N}}(m)(p - 1)2p^{-2m/3}. \]

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

\[ \mathcal{K}_{B_i,m} = \{ (k_1, k_2) \in \mathbb{N}^2 : 3k_1 + k_2 = m \} \]
\[ = \{ (k, m - 3k) : 1 \leq k \leq \lfloor (m - 1)/3 \rfloor \} \]

and we get a summand

\[ M_{B_i,p} \cdot \sum_{k \in \mathcal{K}_{B_i,m}} \prod_{\lambda \in B_i} p^{-(\#\lambda-1)k_\lambda} = (p - 1)^2 p^{-m} \sum_{k=1}^{\lfloor (m-1)/3 \rfloor} p^k. \]
Thus, for \( m \geq 3 \) we have

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

and hence

\[
\mathbb{P}\{\Delta(x) = p^{-n}\} = 1_{3\mathbb{N}}(n+3)(p-1)_2 p^{-2(n+3)/3} + 3(p-1)^2 p^{-(n+3)} \sum_{k=1}^{\lfloor(n+2)/3\rfloor} p^k.
\]
Challenges in the $N \geq 4$ cases

- When $N \geq 4$, there are $B \in \mathcal{R}_N$ with $\#B \geq 3$ and $M_{B,p} > 0$.

- In order to calculate the summand for such $B$, we would need to explicitly describe all elements of

$$K_{B,m} := \left\{ \mathbf{k} \in \mathbb{N}^B : \sum_{\lambda \in B} \binom{\#\lambda}{2} k_\lambda = m \right\}.$$ 

- Even if all $\binom{\#\lambda}{2}$ are relatively prime, this is an open problem!

- For large $N$, it is also challenging to tabulate all $B \in \mathcal{R}_N$ 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 $N \geq 2$

- $M_{B,p} \leq ((p - 1)!)^{N-1}$ for all $N \geq 2$ and all $p$

- $\#\mathcal{K}_{B,m} \leq m^{N-1}$ for all $B \in \mathcal{R}_N$ and all $m \geq \binom{N}{2}$

- If $k \in \mathcal{K}_{B,m}$, then $\prod_{\lambda \in B} p^{-((\#\lambda - 1)k_\lambda)} \leq p^{-\frac{2m}{N}}$

**Corollary**

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

$$\mu^N(\Delta^{-1}(p^{\binom{N}{2}}^{-m})) \leq (2m(p - 1)!)^{N-1}(N-1)!p^{-\frac{2m}{N}}$$
Given $N$ and $p$, there is a positive constant $C(N, p)$ such that

$$P\{\Delta(x) = p^{-n}\} \leq C(N, p) \cdot p^{-\frac{n}{N}} \quad \text{for all } n \geq 0.$$
Thank you!